U.S. Department of Justice

Federal Bureau of Investigation
Washington, D.C. 20535

June 8, 2016

MS. ALEXA O'BRIEN
MUCKROCK NEWS
DEPT MR 17650
POST OFFICE BOX 55819
BOSTON, MA 02205-5819

FOIPA Request No.: 1329099-000
Subject: MAXCAP 05

Dear Ms. O'Brien:

The enclosed documents were reviewed under the Freedom of Information Act (FOIA), Title 5, United States Code, Section 552. Deletions have been made to protect information which is exempt from disclosure, with the appropriate exemptions noted on the page next to the excision. In addition, a deleted page information sheet was inserted in the file to indicate where pages were withheld entirely. The exemptions used to withhold information are marked below and explained on the enclosed Explanation of Exemptions:

Section 552		Section 552a
☑ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☑ (b)(3)	☑ (b)(7)(C)	☐ (k)(1)
50 USC, Section 3024 (i)(1)	☐ (b)(7)(D)	☐ (k)(2)
	☑ (b)(7)(E)	☐ (k)(3)
	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☑ (b)(6)		☐ (k)(7)

71 pages were reviewed and 71 pages are being released.

☐ Document(s) were located which originated with, or contained information concerning, other Government Agency (ies) [OGA].

☐ This information has been referred to the OGA(s) for review and direct response to you.
☐ We are consulting with another agency. The FBI will correspond with you regarding this information when the consultation is completed.

☐ In accordance with standard FBI practice and pursuant to FOIA exemption (b)(7)(E) and Privacy Act exemption (j)(2) [5 U.S.C. § 552/552a (b)(7)(E)/(j)(2)], this response neither confirms nor denies the existence of your subject's name on any watch lists.

For your information, Congress excluded three discrete categories of law enforcement and national security records from the requirements of the FOIA. See 5 U.S. C. § 552(c) (2006 & Supp. IV (2010). This response is limited to those records that are subject to the requirements of the FOIA. This is a standard notification that is given to all our requesters and should not be taken as an indication that excluded records do, or do not, exist. Enclosed for your information is a copy of the Explanation of Exemptions.

For questions regarding our determinations, visit the www.fbi.gov/foia website under "Contact Us." The FOIPA Request Number listed above has been assigned to your request. Please use this number in all correspondence concerning your request. Your patience is appreciated.

You may file an appeal by writing to the Director, Office of Information Policy (OIP), United States Department of Justice, Suite 11050, 1425 New York Avenue, NW, Washington, D.C. 20530-0001, or you may submit an appeal through OIP's FOIAonline portal by creating an account on the following web site: https://foiaonline.regulations.gov/foia/action/public/home. Your appeal must be postmarked or electronically transmitted within sixty (60) days from the date of this letter in order to be considered timely. If you submit your appeal by mail, both the letter and the envelope should be clearly marked "Freedom of Information Act Appeal." Please cite the FOIPA Request Number assigned to your request so that it may be easily identified.

☐ The enclosed material is from the main investigative file(s) in which the subject(s) of your request was the focus of the investigation. Our search located additional references, in files relating to other individuals, or matters, which may or may not be about your subject(s). Our experience has shown when ident, references usually contain information similar to the information processed in the main file(s). Because of our significant backlog, we have given priority to processing only the main investigative file(s). If you want the references, you must submit a separate request for them in writing, and they will be reviewed at a later date, as time and resources permit.

☑ See additional information which follows.

Sincerely,

David M. Hardy
Section Chief
Record/Information
Dissemination Section
Records Management Division

Enclosure(s)

The enclosed documents contained in FBI Headquarters files 62F-HQ-1367274-K8 Serial 14, 66F-HQ-A1300364-K Serial 5, and 66F-HQ-A130871 Serials 11 and 230 represents the final release of information responsive to your FOIA request.

It is unnecessary to adjudicate your fee waiver as there are no assessable fees for the enclosed CD ROM.

This material is being provided to you at no charge.

EXPLANATION OF EXEMPTIONS

SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552

(b)(1) (A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified to such Executive order;

(b)(2) related solely to the internal personnel rules and practices of an agency;

(b)(3) specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld;

(b)(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;

(b)(5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;

(b)(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;

(b)(7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information (A) could reasonably be expected to interfere with enforcement proceedings, (B) would deprive a person of a right to a fair trial or an impartial adjudication, (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy, (D) could reasonably be expected to disclose the identity of confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of record or information compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source, (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or (F) could reasonably be expected to endanger the life or physical safety of any individual;

(b)(8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or

(b)(9) geological and geophysical information and data, including maps, concerning wells.

SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552a

(d)(5) information compiled in reasonable anticipation of a civil action proceeding;

(j)(2) material reporting investigative efforts pertaining to the enforcement of criminal law including efforts to prevent, control, or reduce crime or apprehend criminals;

(k)(1) information which is currently and properly classified pursuant to an Executive order in the interest of the national defense or foreign policy, for example, information involving intelligence sources or methods;

(k)(2) investigatory material compiled for law enforcement purposes, other than criminal, which did not result in loss of a right, benefit or privilege under Federal programs, or which would identify a source who furnished information pursuant to a promise that his/her identity would be held in confidence;

(k)(3) material maintained in connection with providing protective services to the President of the United States or any other individual pursuant to the authority of Title 18, United States Code, Section 3056;

(k)(4) required by statute to be maintained and used solely as statistical records;

(k)(5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment or for access to classified information, the disclosure of which would reveal the identity of the person who furnished information pursuant to a promise that his/her identity would be held in confidence;

(k)(6) testing or examination material used to determine individual qualifications for appointment or promotion in Federal Government service he release of which would compromise the testing or examination process;

(k)(7) material used to determine potential for promotion in the armed services, the disclosure of which would reveal the identity of the person who furnished the material pursuant to a promise that his/her identity would be held in confidence.

FBI/DOJ

b6
b7C

• *Prepared by:* [redacted] *C7D*
10.08.02

Counterterrorism Reprogramming

- The FBI's reorganization reprogramming of $202,301,000, approved by Congress on July 31, 2002, shifts $86,786,000 from criminal programs, of which $73,517,000 is dedicated to the FBI's counterterrorism program.

- Centralized Management of CT Investigations - The Assistant Director for Counterterrorism is responsible for national program management of cases and operations within the program and for a select number of cases and operations which require national-level management due to special circumstances, situations, or sensitivity. A characteristic of Counterterrorism cases is that they are often national in scope. Individual field offices often deal with only a segment or portion of a larger investigation that often transcends field office territorial boundaries and even national borders. Centralized management of these cases is needed to ensure the individual pieces of the investigation can be assembled into a coherent picture.

- Under the leadership of Dale Watson, Former Executive Assistant Director of Counterterrorism and Counterintelligence, the FBI developed a strategic plan to position the FBI in the best proactive stance to counter the threat of international terrorism by 2005. (MAXCAPOS) The main focus of this initiative was not cases, which are by definition reactive, but rather about knowing the environment and creating tools to aid decision-makers, fostering accountability, consistency and accuracy among FBI Executive Management regarding understanding and countering the terrorist threat.

- Under this plan, the definition of maximum feasible capability included five natural elements:
  - **Investigative Capacity** - the extent to which each FBI field office is appropriately staffed, trained, equipped and managed to prevent and effectively respond to acts of terrorism.
  - **Intelligence Capacity** - the extent to which the FBI can provide information and intelligence of value and support to field investigations by developing a program focused on identifying and filling existing intelligence gaps.
  - **Communications Capacity** - focuses Bureau resources on the critical security considerations and technology needed by the CT Programs to communicate effectively and efficiently.
  - **Liaison Capacity** - the ability to establish and maintain sound and productive relationships with external counterparts in the intelligence community, law enforcement communities, other federal agencies, defense establishments, foreign services, private industry and nongovernmental organizations, state and local agencies, legislative and executive bodies, the media and academia to obtain maximum information and support.
  - **Program Management Capacity** - capacity of the HQ Program managers to use all necessary assets and capabilities to support and initiate complex CT operations designed to penetrate and neutralize terrorist threats.

~~LAW ENFORCEMENT SENSITIVE~~

STRATEGIC PLANNING IN
THE COUNTERTERRORISM DIVISION

MAXCAP05

August 1998 to September 2001

Counterterrorism Working Group

The first meeting of the Counterterrorism Working Group (CTWG) was held on March 28, 2000- While there was no written agenda, it was clear that Dale Watson, the newly named Assistant Director (AD) for the Counterterrorism Division (CTD) had a plan. He had been working with several close advisors since the 1998 bombings of the American Embassies in Kenya and Tanzania on a new approach to managing the FBI's Counterterrorism (CT) Program and now, as newly named AD, he was ready to put this new vision into action.

The team assembled included unit cmef-level representation from each of the four components of the CTD at FBIHQ: International Terrorism (IT); Domestic Terrorism (DT); the National Infrastructure Protection Center (NIPC); and the National Domestic Preparedness Office (NDPO). Also in attendance that first day were one planning advisor and two representatives from the Finance Division (FD) planning staff.

AD Watson explained that since KENBOWRANBOM, he had been seeking a mechanism which would move the CT Program from a reactive posture towards a more proactive approach to counterterrorism. Together with his colleagues in CTD, AD Watson developed a comprehensive strategy which would improve the ability of the counterterrorism community to both prevent and respond to terrorist acts around the world.

Defining Capacity

AD Watson articulated his fundamental guiding principle: the FBI will never be able to prevent all acts of terrorism. This premise, which is based on the political social and economic realities of terrorism allowed AD Watson to entirely rethink the way the FBI's CT Program is managed. By acknowledging the limits fo even the most capable program, AD Watson initiated a shift in how to approach the CT Program, crating opportunities for innovative strategic thinking. Accepting that there will always be limits to the FBI's ability to stop all terrorist acts, the traditional indicators used to measure success in the CT Programs (arrests, convictions, terrorist acts prevented, etc.) have little utility.

Instead, AD Watson reasoned that the best approach to managing the CT program is to focus on building maximum feasible capacity in all areas of the program. The new strategy, therefore, consists of. defining maximum capacity; assessing current capacity; identifying gaps in capacity; and developing tactics for addressing those gaps. The heart of this strategy lies in intensive, consistent internal assessment. To implement this management strategy, the CTWG needed to review existing program management tools and

develop new tools as necessary to ensure that the CTD has the ability to conduct comprehensive assessments.

To structure the definition of maximum feasible capability, AD Watson articulated the program's five natural elements: **Investigative Capacity, Intelligence Capacity, Communications Capacity, Liaison Capacity, and Program Management Capacity.** These components became known as the CT Program's Five Levels. The initial work of the CTWG focused on specifically defining what maximum capacity looks like in each of the Five Levels. Once capacity is defined, program managers have a road map for success and a bar against which to measure progress toward maximum feasible capacity.

[For an in-depth discussion of the Five Levels, please refer to Appendix A.

Communications

Along with the CTWG, AD Watson created a CM SAC Advisory Board. This Board, made up of five FBI SACs from across the country, provided input, feedback, and suggestions throughout the process of defining capacity. Their participation not only provided a valuable field perspective to the planning process, but also granted legitimacy to the initiative by ensuring early buy-in from senior field office managers.

Further field management buy-in was achieved through four regional SAC conferences held in the summer of 2000. Ile key to the success of these conferences was that they involved SACs in the process of defining capacity. AD Watson's planning proposal achieved an unprecedented level of field-wide support because it was presented to the SACs while it was still a work-in-progress and, therefore, open to review and input. One example of the participatory nature of the process was the development of a time frame for achieving maximum feasible capacity. Given the SACs file reviews of the CT program in their Divisions, which were completed at the regional conference, CT managers realized that the achievement of maximum feasible capacity was possible by FY 2005. This time frame became the explicit goal of the CT planning initiative and, subsequently the CT planning initiative was named MAXCAP 05.

[For an in-depth discussion of the MAXCAP05 communications strategy, please refer to APPENDIX B.

Accountability

Of all the program management tools that the CWG reviewed, mechanisms for holding program managers accountable for progress towards maximum feasible capacity were a priority. The CT'WG found that there were some systems in place (e.g. AFOR, Program Plans, SAC Conference Calls) that could be easily adapted for use with MAXCAP05. These mechanisms are part of the overall strategic planning system at the Bureau and their development was driven by the Government Performance and Results Act (GPRA) of 1993, which requires government agencies to set goals and objectives and to track progress towards their completion. The C'IVG worked with the Bureau planning staff to integrate MAXCAP05 into already existing accountability tools, strengthening both MAXCAP05 and Bureau planning in general In other cases entirely new

systems needed to be created (e.g. Director's Report on Counterterrorism). Management's accountability is emured, therefore, through several mutually-reinforcing mechanisms.

Investigative Capacity (Level 1): Investigative Capacity is primarily focused on field functions, therefore the mechanisms for accountab&y focus on the SAC.

- The Annual Fleld Office Report (AFOR) is the mechanism througb which the field answers all HQ reporting requirements for the year, from resource needs to threat assessments. Biannually, the Deputy Director conducts SAC Conference
- Calls with the executive management of each Field Division. These phone calls are traditional mechanisms that are closely tied to SAC PARs and have been easily incorporated into MAXCAP05.
- The Director's Report on Counterterrorism is a bi-annual comprehensive reporting document that summafim all levels of the national Cr prograril M-ds is one of the new tools developed specifically for MAXCAP05 implementation. The Director's Report is available to FBIHQ senior management for use in policy-maldng, national program management, and resource allocation.
- Field Divisions are inspected every three years. The CTD works with the Inspection Division to focus the CT portion of inspection assessments on the elements of capacity, as defmed by CTD).

- Intelligence Capacity (Level 2): Much of the responsibility for intelligence and analysis lies outside the CTD, making accountability in this area more challenging.
- CTD has proposed an intelligence pilot project, which would establish a system to clearly delineate CTD's intelligence needs to the Investigative Services Division (ISD) through Priority Information Requests (PIRS) and to work with ISD to address intelligence gaps.
- The FBIFIQ equivalent of the AFOR are the CTD Program Plans. Just as the SACs are responsible for the content of the AFORS, CT7D Section Chiefs are responsible for the content of annual program plans. These plans lay out goals, objectives, and performance indicators for the year, as well as any CTD requirements for other HQ Divisions. Like the AFOR, Program Plans preceded MAXCAP05 and have been a -useful tool for CTID's strategy.
- As with all five levels, progress towards maximum capacity is reported biannually in the Director's Report.

Communication Capacity (Level 3): Again, much of the responsibility for communication lies outside the CTD.

- The CTD will work with the Information Resource Division (IRD) to fully integrate MAXCAP05 into Trilogy.
- FBIHQ has included the unblocking of case files as a Level I criteria to encourage maximum information sharing.
- Level 3 is also addressed and accounted for through the annual CTD Program Plans.
- Again, progress towards Conununications Capacity.is reported in the Director's Report on Counterterrorism.

Liaison Capacity (Level 4): Responsibility for haison falls both within and without the CTD and at both HQ and in the Field.

Inside CTD, development and maintenance of key partnerships is primarily the responsibility of CTD Sections, therefore, accountability focuses on the Section Chiefs. Outside CTD, the CT Program is dependent on FBIHQ Support Divisions (e.g. OPCA, Finance, etc.) for maintenance of the external liaison necessary for success.

- Level 4 is also addressed and accounted for through the annual CTD Program Plans.
- The CTD equivalent of the SAC Phone Calls is the Section Chief Contracts. Like the
  Like the Director's Report, this is a newly developed accountability mechanism which holds the Section Chiefs accountable for progress towards maximum capacity.

Program Management Capacity (Level 5): Due to the all-encompassing nature of the capacity covered in Level 5, all of the accountability mechanisms previously described contribute to the tracking of accountability for program management in Level 5. CTD Program Plans, in that they represent the product (program strategy) of Level 5, are also accountability mechanisms for Level 5 to the Deputy Director. Ultimate responsibility, however, lies with the AD, thus this level includes the use of another

previously-established accountability mechanism, the AD Contract. This contract is updated annually and is agreed upon by the AD and the Deputy Director. The products of the Level 5 process are the CTD Program Plans, which address all levels and include Program priorities and investigative/intelligence strategies.

[For an in-depth discussion of accountability, please refer to APPENDIX C, for an in-depth discussion of the Director's Report and AFOR, please refer to APPENDIX D; and for an in*depth discussion of the intelligence pilot, please refer to APPENDIX F.]*

Staffing and Budget

As previously mentioned, in October of 1999 the FBI undertook a major reorganization. The centerpiece of this reorganization was the creation of two new divisions, the Investigative Services Division (ISD) and the(CTD). AD Watson saw the reorganization as an opportunity to explore creative approaches to staffing which would more efficiently serve the new strategy.

When the CTD was first established, it was organized in the traditional FBI mold with Units, Sections, a Deputy Assistant Director (DAD), and an AD. The CTWG began as early as March of 2000 looking at alternatives, particularly movement away from the existence of "mini-headquarters within the CTD. AD Watson was concerned with the decentralization of effort from having units inside CTD and in other Divisions that contribute to the same functions (e.g. budget, staffing, technical support, security, etc.). Operational divisions bad established their own support functions because they were not getting the full specialized support they needed from the service divisions, but AD Watson and the CTWG wanted to explore the possibility of developing specialized program services within the support divisions to maximum efficiency. Given the extent to which the mini-headquarters arrangement has become ingrained into the operations of FBIHQ, change in this arena has proved to be challenging, but progress is being made. All computer support functions have been moved back to the Information Resources Division (IRD) and all personnel functions have been moved back to the Administrative Services Division (ASD). Next the CTD will work with the Finance Division (FD) to consolidate budget and financial functions.

CTD communicates with support divisions in two ways. First, CTD has established an Executive Staff which services the IT, DT, and NDPO programs (NIPC has a separate, similar office). The role of these staffs is in transition. At the moment, they continue to provide limited support services to the CTD, but they are moving toward a coordination role with the service divisions. Second, each CT program is working on their own to be more explicit about their requirements from support divisions and to articulate these needs through the annual Program Plans.

Since the heart of MAXCAP05 is intensive internal assessment, managing the process is labor intensive. The CTWG quickly recognized that work on MAXCAP05 would not only need the assistance of the service divisions, but would also require a small, permanent planning staff that reports directly to AD Watson. This stafrs primary responsibility will be to ensure that the numerous mechanisms associated with MAXCAP05 are functioning properly. Additionally, the staff will focus on interpreting the. multiple assessment tools into a form that is accessible to executives for us ' e in policy and program management. A planning staff is also important to ensure that program planning work is managed at the highest level of C7D executive management and that CT performance is accurately and effectively reported to oversight entities and the American people. While the strategy development process has benefitt ' ed greatly from the dynamic leadership of AD Watson, a permanent staff reporting directly to the AD will help institutional planning as a critical element of executive management in the future. This planning staff has not yet been established and discussions are ongoing.

All of the program management tools used by the CTD to assess capacity also enable managers to evaluate resource needs more accurately and to justify resource requests more fully. Ile consistency produced by systematic assessment makes the budget process easier and more connected to the CT program's strategy. Recognizing these additional benefits of MAXCAP05, CTD moved expeditiously to utffiw assessment results in budget formulation, justification, and allocation. While this greatly improved the budget process, it also presented new challenges, primarily the clear communication of the strategy to oversight entities. The change tbzit the CTD is pursuing in the budget process requires a basic understanding of the principles of MAXCAP05. Due to the many partners involved in the budget cycle (e.g. DOJ, OMB, Congress, etc.), bringing everyone to a common understanding is an effort that will take time and consistent communication.

[For an in-depth discussion of staffing and budgeting, pkase refer to APPENDIX E.]

Minding the Gaps

Now that a system for ongoing, meaningful assessment has been put in place, the CT Program is in the process of focusing its resources on mending the gaps in capacity which have been uncovered through the assessment process at every level of the progranl Prioritizing these next steps towards achieving maximum capacity is critical Not only will clear priorities help focus CID's efforts, but it will also allow CTD to clearly articulate to its partners, both inside and outside the FBI, the areas in which the CT program needs priority assistance in its efforts to reach maximum feasible capacity. Gaps can be defined as systemic, organizational, and operational

Systemic Gaps

Both before and after capacity assessments were conducted, it was clear that the main gaps in the CT Program are training, translation, and analysis. Projects are underway in all three of these areas.

In the area of training, CTD has assigned a full-time coordinator to ensure that the Training Division fully supports the priorities of the CT program and helps to fill the gaps indicated by capacity assessments both in Field Divisions and at FBUIQ. Training initiatives in development include adjustments to New Agent Training, specialized in-services, distance learning programs, and a working group on strategic planning.

Translation has been an issue since the beghming of the CTD planning initiative and discussions have included faster clearance times for applicants and the possible creation of a Language Center to centrahw translation capabihfies. After the September 11 attacks, the Dirmor issued a request to the public for translators and the Bureau has received many applications. Currently, translators are working through the backlog of [redacted] background investigations on translator applications have been prioritized and streamlined, and discussions continue about moving translation capabilities to an off-site location. Improving the FBI's translation capacity is one of the Director's highest priorities. b7E

Efforts to improve analysis have focused on better coordination between the CTD and the ISD, including articulating CT program needs though Program Plans and Priority Intelligence Requirements (PIRs). The CTD has proposed an intelligence pilot designed to produce timely and useful intelligence products that are focused on priority investigative objectives. The pilot project will focus on:

- Identifying PIRS;
- Analyzing available information and identifying intelligence gaps;
- Collecting information needed to close intelligence gaps;
- Reportmg and mtegratmg mtelhgence mto mvestigauons; and
- Evaluating the intelligence in terms of utility to the field.

Organizational Gaps

There are also a number of organizational gaps which need to be addressed in order to achieve maximum feasible capacity, including:

- Implementation of Trilogy.
- Planning Staff.
- Executive Staff.

- Performance Measurement Reporting.

Operational Gaps

In terms of operational next steps, the CTD executive level meetings-in **FYO1** (as required by Level 5) produced program plans for each of the four CT programs, which outline operational priorities.

[For an in-depth discussion of Minding the Gaps andfor a summary of the operationalpriorities for IT, DT, NIPC, and NDPO, please refer to APPENDIX F. I

Conclusion

The terrorist attacks on September 11, 2001 do not change CTD's MAXCAP05 strategy. Indeed, the attacks intensify and further demonstrate the need for comprehensive program management that systematically identifies and addresses capacity gaps. Since the FBI cannot prevent an acts of terrorism, the CT Program cannot say definitively that had MAXCAP05 been fully implemented before September I 1, the attacks would have been prevented. Full implementation, however, puts the FBI in the best possible position to prevent, detect, deter, and defeat terrorism. The progress made by the CTD already puts the FBI in a better position to investigate the events of 09/11/01 and to prevent further attacks. Since CTD has already conducted a comprehensive assessment of capacity and has thoroughly identified and documented capacity gaps, the FBI is in a good position to use the renewed interest in counterterrorism and the funding increases anticipated in the near future to direct resources and attention where they are most needed and can be most effective.

The CTD is two years into the MAXCAP05 effort and still plans to have the initiative in place by 2005. The CTD believes that the pursuit of maximum feasible capacity is the best strategy to counter the terrorist threats facing the U.S. and U.S. interests and will pursue full implementation of MAXCAP05as one of the Division's top priorities.

Definition of maximum feasible capacity can be achieved by breaking the effort down into five manageable pieces, referred to as five levels of capacity. Within each level, each program has identified specific criteria that, when taken together, represent maximum capacity in that level. These criteria provide a specific plan of action that program mangers can use to prioritize and organize the program in pursuit of maximum feasible capacity. 'Me criteria are reviewed continuously to account for progress and new requirements or issues. - Once the criteria are defined for each level, program managers'responsi@ and priorities become clearly defined. Each level is highly dependent on and interrelated with the others.

Capacity within each level is expressed using a red/, rating system. Red indicates that there are significant vulnerabilities with serious problems continuing; yellow indicates that there are significant vulnerabilities, but progress is being made to resolve the gaps; and green indicates maximum feasible capacity. While the assigm-nent of a color rating is to some extent a judgermnt call, it is supported by the specific criteria within each level. Managers justify the capacity ratings given progress towards each criteria, and can clearly define which criteria accounted for the final rating, there by indicating areas of priority emphasis. It is not the color rating itself that is the most helpful aspect of capacity assessment, although the colors do provide a useful overview of the CT prograim. The most important part of capacity ratings is the process of assessment itself and the conversation about the criteria that determine overall color ratings. It is through this process and conversation that program managers can best see where the program is and where it needs to go. While the color ratings are a good sununary tool, the most significant product of this assessment process is a clear, prioritized road map for action.

Investigative Capacity is located in the Field Office, therefore, responsibility for Level I lies with the

Level 1, Investigative Capacity, is the extent to which each FBI FwM Office i-s appropriately staffed, trained, equipped, and managed to prevent and effectively respond to acts of terrorism.

SAC of each Field DivisiorL The SAC oversees the APOR process and, based on the input provided by CT managers in the field, makes the final decision on capacity ratings for the four CT programs, as well as for the CT effort as a whole in that particular Division. Any dfferences of opinion between field and HQ components as to what capacity ratings should be reported are resolved through discussions between the SAC and the AD. CTI) executive management recognizes that many of the staffing, training, and equipment issues that may cause a Field Division to be - or red are often the responsibility of HQ entities as well. SACs are only responsible for those elements of capacity that they can control, but are also responsible, for clearly corrumunicating issues beyond their control to HQ through AFORs and discussions of capacity ratings so that program managers and SACs can work together to close capacity gaps.

The field data used to evaluate capacity for each Field Office are gathered every year through the AFOR and are reported to senior management through the Director's Report on Counterterrorism. In addition, the capacity information gathered from Field Offices is used to make staffing and budgeting decisions. Level I is the best developed level thus far, and is supported by SACs throughout the Field. While improvements continue as CID management develops a more thorough picture of capacity, the last AFOR/Director's Report cycles have been very successful and are well on the way to

institutionalization.

Responsibility for intelligence is divided among HQ components. CM Sections, in co ' ordination with ISD, are responsible for evaluating intelligence capacity, again reporting red ratings through the Director's Report. CTD Program Managers base their assessment of Intelligence Capacity on the

Level2, Intelligence Capacity, is the extent to which the FBI can provide information and intelligence of value and support to field investigations by developing a program focused on identifying and filling existing intelligence gaps.

identified intelligence gaps and the ability of the FBI to meet the established priority information requirements (PIRs). The overall assessment of Level 2 also takes into account the individual intelligence base assessment conducted by each Field Office in Level 1, communications effectiveness in Level 3, and liaison effectiveness in Level 4. Level 2 is in the beginning stages of impkn=tation.. PIRs have been developed by CTD for ISD and an intelligence pilot has been proposed for closing intelligence gaps and institutionalizing a process by which CTD and ISD work together on analytical requirements.

[For an in-depth discussion of the intelligence pilot project, please refer to APPENDIX F.

Communications Capacity is also managed at FBIHQ and the Tesponsibility for effective communications lies throughout the Bureau. The Level 3 assessment considers policy development, systems implementation, infrastructure connectivity, equipment, and system evaluation. Given in this level means that

> Level 3, Communication Capacity, focuses Bureau resources on the critical securityconsiderations and technology needed by the CT programs to communicate effectively and efficiently.

all Field Offices, Resident Agencies, and HQ entities have the capacity to exchange information and intelligence and to recover critical data and records smoothly and comprehensively. It also means that all internal entities involved in the CT effort are on the same page about priorities and strategies to close capacity gaps. CTD Sections, in conjunction with all other internal entities, evaluate and report Level 3 capacity through the Dhwtor's Report. Level 3 is also in the beginning stages of implementation. CTD anticipates working with IRD on the Trilogy initiative to improve connectivity and communication throughout the Bureau. Trilogy is a three-year initiative that will upgrade the FBI's aging computer infrastructure and will convert investigative and intelligence applications to the new web-based architecture. The intent of Trilogy is to integrate throughout the FBI a common set of easy-to-use applications to access and provide basic analytical capabilities for investigative and intelligence information that may include text, imagery, audio, and video formats, and to provide these capabilities regardless of the physical location of FBI investigators and analysts. IRD plans to involve user representatives at every phase during the Trilogy implementation period to ensure that the project continues to focus on meeting user needs. The Intelligence Pilot discussed in Level 2 will also help develop continuous communication between FBI components.

[For an in-depth discussion on the intelligence pilot, please refer to APPENDIX F.]

While liaison with external counterparts occurs both in the field and at FBIHQ, responsibility for managing and assessing liaison capacity lies at Headquarters. As with Intelligence Capacity, the assessment

Level4, Liaison **Capacity,** is the ability to establish and maintain sound and productive relationships with external counterparts in the intelligence community, law enforcement communities, other federal agencies, defense establishments, foreign services, private industry and nongovernmental organizations, state and local agencies, legislative and executive bodies, the media, and academia to obtain maximum information and support.

of Liaison Capacity takes into account assessments provided by each Field Office through the AFOR on their own liaison capacity. Liaison at FBIHQ consists of. 1) identification of partners; 2) establishment of relationships; 3) mutual needs assessments; 4) information sharing; and 5) joint project development. CTD Sections, in conjunction with other relevant partners, evaluate Liaison Capacity and assign color ratings that are reported through the Director's Report. While the CT Program continually works to improve liaison relationships, this is the level in which capacity is currently the highest. Relationships with external partners are, in general, good and continue to improve.

Level 5 is critical to the CTD Strategy, as it ties all levels together into clearly articulated, prioritized, monitored goals, objectives, and proactive strategies, which in turn are articulated in the Program Plans.

Level 5, **Program Management Capacity,** is the capacity of HQ Program Managers to use all necessary assets and capabilities to support and initiate complex CT operations designed to penetrate and neutralize **terrorist** threats.

Program Management Capacity draws on the capabilities of the other four levels and identifies national program and operational objectives **that** constitute the most critical priorities for the FBI's CT Program. Following the annual assessment of the first four levels, each of the FBIHQ CT operational Units prepares the program objectives for the specific national CT program managed by that Unit. Each of the objectives are prioritized and are accompanied by a plan to address each objective on a national level Upon completion of

the Unit priority objective meetings, the AD meets with each Section program manager responsible for developing the goals and objectives, which are based on the goals and objectives of each Unit. The AD then forms the CTD's national priorities based on those goals and objectives identified by the Sections. These objectives will target the most significant threats to U.S. national security in the CT arena. In addition to Program Plan development, the Level 5 process of decision-making and prioritizing may also be manifested in intelligence and operational products on particular threats and issues. For example, CTD and ISD have been working on a comprehensive threat analysis and strategy document for ALF/ELF. Such products support the Program Plans and provide additional guidance at both FBIHQ and in the Field about CTD operational and intelligence priorities and strategies.

In essence, **Levels 1-4 produce information about the program and Level 5 processes that information.** The products of this Level 5 process are the Program Plans (and other related strategy documents), which reticulate -the investigative and intelligence priorities and strategies for the year. -ne Program Plans include the national direction of each program, goals and objectives, and actions required to meet these objectives. **MAXCAP05 is a program management strategy that facilitates and informs the development of operational strategy.**

This systematic development of national priorities allows the FBI to focus national resources on threats with the

highest potential impact on the U.S. and its interests. Upon the identification and prioritization of national objectives and plans, CID management has the opportunity to surge on a priority threat This surge would focus specific investigative resources on an identified terrorist activity for a specified period of time to cause a significant disruption or prevention of the identified terrorist operation.

[For an in-depth discussion of Accountability, please refer to *APPENDIX C, for* an *in-depth discussion of the AFOR and Director's Report on Counterterrorisn4 please refer to APPENDIX D; and for an indepth discussion of Staffing and Budgeting, please refer to APPENDIX E.]*

Example:.Five Level Applicability to ALF/ELF
(sample for demonstration purposes only)

The following example demonstrates how the Five Levels could apply to a particular threat or investigation. This analysis is intended as a sample only to facilitate understanding of the five levels and does not represent actual current efforts in the DT Section. While the AFOR reporting in Level I is drawn directly from the 2001 AFOR, the rest of the example is fictional

Level 1: b7E

Level 2 b7E

b7E

- b7E
-
-
-
-
-
-
-

- [redacted] b7E
- [redacted]

Level 3: [redacted] b7E

[redacted]

[redacted] b7E

Level 4: [redacted] b7E

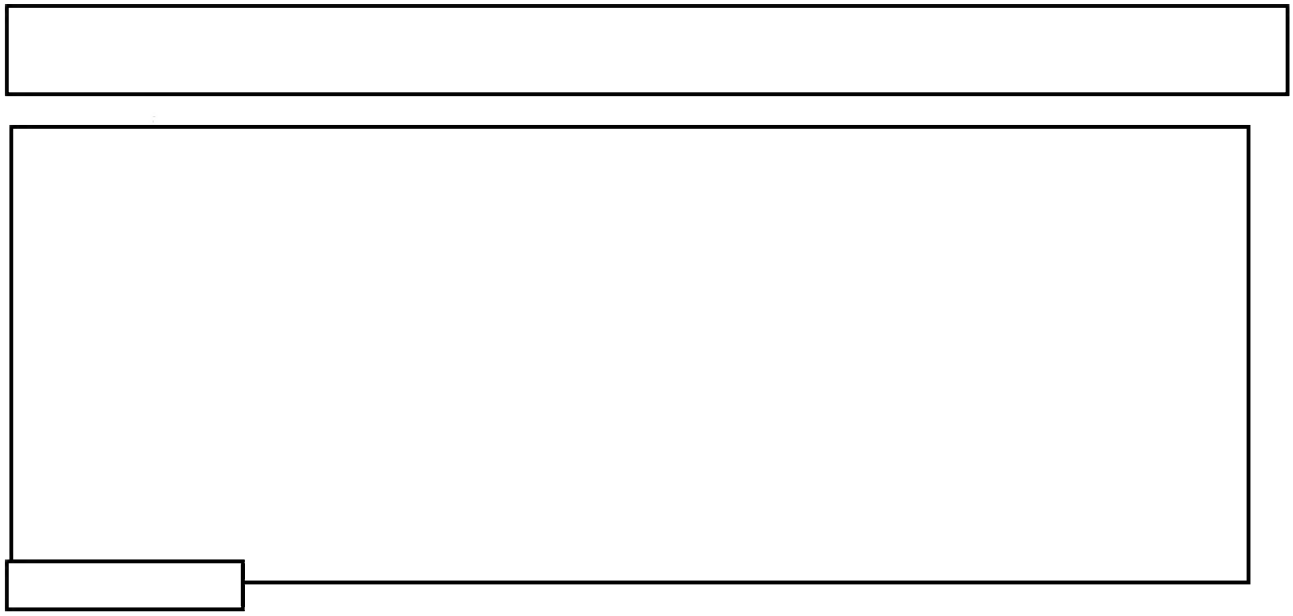
[redacted]

- [redacted] b7E
- [redacted]
- [redacted]
- [redacted]

Level 5: [redacted] b7E

[redacted]

- [redacted] b7E
- [redacted]
- [redacted]
- [redacted]



b7E

b7E

As demonstrated by this example, the five levels are highly interactive and overlap significantly. This is intentional to allow for maximum national coordination against terrorism and to create, in essence, a network that can quickly recognize. assess, and act against dimts.

Again, this example is fictional account to demonstrate how the Five Levels function and is not intended to represent the current situation or current CTD strategy.

CTD SAC Advisory Board

Along with the CTWG, AD Watson created a CTD SAC Advisory Board. The Board, made up of five FBI SACs from across the country, provided input, feedback, and suggestions throughout theprocess of defming capacity. Their participation not only provided a valuable kield perspective to the planning process, but also granted legitimacy to the initiative by ensuring early buy-in from senior field office managers.

T'he CTD SAC Advisory Board reviewed the criteria for the Five Levels as the CTWG developed them, providing helpful insight, ideas, and suggestions. This Board was available to the AD as a resource that was fully informed about MAXCAP05, had extensive working knowledge of FBI operations and management, and had both Field and HQ experience. 'Me SAC Advisory Board was also very helpful during the SAC Conferences (see below) by volunteering to provide exwnples of Level I assessments to demonstrate to other SACs how the capacity ratings work. Getting buy-in and participation from these few SACs from the beghming of the initiative proved to be critical in developing a comprehensive program and in explaining the system to the rest of the field. Incorporating field management early on also helped to mitigate the inevitable suspicion of

significant change and of strategic planning, making the CID's case even stronger.

SAC Conferences

Over the summer of 2000, the CTD sponsored four regional SAC conferences to explain the five level strategy and the details of Level I reporting to the SACs and to get their input and suggestions. The conferences were very successful, generating praise and useful discussion.

At the conference, AD Watson presented the management initiative to the group, explaining effort developed. Each SAC then went through a series of worksheets walking them through the criteria developed for Level 1 and allowed them to make a preliminary assessment of the counterterrorism program in the Division. The SAC of the host office allowed their self-assessment to be shared and discussed as an example before the other SACs completed their own assessments. Other SACs volunteered their conclusion, but this exercise was fro demonstration only and they were not required to share ratings. Through this exercise, SACs were able to see exactly how the system works, what is expected of them as managers, and how they would be held accountable for their officer's capacity. In addition, they were able to give specific suggestions on the criteria and what would make the process easier and more effective for everyone.
in their Division. 'Me SAC of the host office allowed their selfassessment to be shared and discussed as an example before the

The SACS had a number of helpful comments and brought up important issues to be addressed for the initiative to work. Recurring themes included:

- Reporting red/green assessments out to external entities and exactly how these assessments will be used.
- Maintaining consistency among executive management across the CTD and the FBI as a whole.
- Securing and maintaining the support of the Deputy Director
- Addressing the translation problem.
- Using this process to improve the budget process.
- Improving the relationship between operational and support divisions.
- Improving relationships with other agencies.
- Improving analytical support.

The reaction to the initiative was overwhelmingly positive, if somewhat tempered at times by cynicism that FBIHQ can make this happen. OveralL however, MAXCAP05 has the full support of the field, which is critical to the project's ultimate success.

The CTD will plan further SAC conferences as necessary. The Program will track new SAC appointments and when there are enough SACS who have not had the opportunity to be briefed on and provide input on MAXCAP05, the CTD will hold another conference. Similarly, the CTD will ensure that other senior field and HQ managers are briefed and their input solicited regularly. 'Me CTD will also keep the Dhwtor and Deputy Director fully informed, as well as maintain continuous liaison with Department of Justice executives, budget staff, and planning Staff.

Appendix C
Accountability

Mechanisms for accountability are driven both internally and externally. Internallly, the CTWG and the AD recognized early in the process that the success of MAXCAPOS depended on executive management's ability to hold managers throughout the Bureau responsible for the criteria articulated in each level Without incentives, both in terms of accountability and the budget, change would be difficult Externally, oversight agencies (DOJ, OMB) and the Congress were urging government agencies to improve performance and performance tracking. In 1993, Congress passed the Government Performance and Results Act (GPRA) requiring agencies to set goals and objectives and to accurately track progress towards these goals. _' GPRA provided the incentive for the development of many of the mechanisms for accountability that preceded MAXCAP05 and were adapted for use in CTD's program management strategy. In addition, MAXCAP05 facilitates tracking of progress towards the goals and objectives in the Attorney General's Five-Year Interagency Counterterrorism Plan. In sum, a mutually reinforcing web of accountability mechanisms satisfies both CTD management's desire to continually track progress towards maximum feasible capability and the desire by external agencies to ass'ure performance in government agencies and programs.

Level I (Investigative Capacity): Investigative Capacity is primarily a field function, therefore the mechanisms for accountability focus on the SAC.

- The AFOR is the mechanism through which the field answers aU HQ reporting requirements for the

year, from resource needs to threat assessments. *[For an in-depth discussion of the AFOR, please refer to APPENDIX D.]*

- Biannually, the Deputy Director conducts SAC Phone Calls with each Field Division. These phone calls are traditional accountability mechanisms that are closely tied to SAC PARS. The SAC Phone Calls give the Deputy Director the opportunity to stay informed about what progress is being made and what problems may exist in Field Divisions. SAC Phone Calls were conducted before MAXCAP05, but since the CTD strategy has been developed, Level I mechanisms have been incorporated into the discussion. When the Deputy Director and SAC talk about the Cr Program in a particular Division, it is understood that they address progress and issues in terms of the criteria developed for Level 1. The color rating system is used in the phone calls and any changes in capacity from year-to-year are di!.::cussed. Pulling MAXCAP05 into the SAC Phone caus ftirther reinforces the priority of the initiative and provides the CID with an additional tool to track progress and ensure accountability.
- The Director's Report on Counterterrorism is a bi-annual comprehensive reporting document that summarizes all levels of the national CT program. This is one of the new tools developed specifically for MAXCAP05

implementation. The Director's Report is available to FBHIQ senior management for use in policy-making, national program management, and resource allocation. [For *an in-depth discussion of the Director's Report, please* refer *to APPENDIX D.]*

- Field Divisions are inspected every three years. The CTD has worked with the Inspection Division to focus the CT portion of **inspection assessments** on the elements of capacity, as defined by CTD. Two field office inspections have been conducted using CTD's Level 1 criteria and preliminary feedback indicates that the process went well. Next steps in this area include institutionalizing a mechanism for resolving any disputes that may arise between field Divisions, Inspectors, and the AD.

Level 2 (Intelligence Capacity): Much of the responsibility for intelligence and analysis lies outside the CTD, making accountability in this area more challenging.

The FBIHQ equivalent of the AFOR are the **CTD Program Plans.** Just as the SACs are responsible for the content of the AFORS, CTD Section Chiefs are responsible for the content of annual program plans. Ilese plans lay out goals, objectives, and performance indicators for the year, as well as any CTD requirements for other HQ Divisions. Like the AFOR, Program Plans preceded MAXCAP05 and have been a useful tool for CTD's strategy. Program plans are coordinated from the Office of Strategic Planning, which is overseen by **the** Deputy Director. The plans are requirements for all Bureau programs, both operational and support, and are connected to the Bureau-wideStrategicPlan. Program Plans are one of many resources used to form budget requests and performance reports to external oversight, as they identify gaps in programs, the steps and resources necessary to fill these gaps, and the national direction and priorities of the program. In the C'fD, the Program Plans for the four components are all based on MAXCAP05 and have evolved into a useful internal management mechanism for CT managers, as well as another tool for reporting progress, in this case to the Deputy Director's Office. The Program Plans are the product of Level 5, then feed back into each of the other four levels as a mechanism for communicating with the field,

setting forth the national direction of the program, establishing and communicating CrD priorities, establishing and communicating operational guidance, and holding program managers accountable to the Deputy Director.

- CTD has proposed a system which clearly delineates CTD's intelligence needs to the **investigative Services Division (ISD)** through CT **Px-ogram Plans** and **Priority Intelligence Requirements (PMs).** *[For* an in-depth discussion of coordination *with* ISD on ***intelligence and analysis,*** *please refer* to *APPENDIX F.]*
- As with all five levels, progress towards maximum capacity is reported biannually in the Director's Report.

Level 3 (Conununication Capacity): Again, much of the responsibility for communication lies outside the CTD.

- The CTD will work with IRD to fully integrate MAXCAP05 into Trilogy. Trilogy is a three-year initiative that will upgrade the FBI's aging computer infrastructure and will convert investigative and intelligence applications to the new web-based architecture. The intent of Trilogy is to integrate throughout the FBI a common set of easy-to-use applications to access and provide basic analytical capabilities for investigative and intelligence information that may include text, imagery, audio, and video formats, and to provide these capabilities regardless of the physical location of FBI investigators and analysts. IRD plans to involve user representatives at every phase during the Trilogy implementation period to ensure that the project continues to focus on meeting user needs.
- Communication issues and requirementstguidehnes for working with other HQ Divisions are also addressed in the CTD Program Plans.
- FBIHQ has incorporated the unblocking of case files as a Level I criteria to encourage maximum information sharing. VAME there are specific instances in which access to cases should be restricted, CTD wants to ensure that as much information as possible is made available throughout the FBI so that relevant connections between cases can be identified and exploited quickly. Limiting blocking to very specific reasons is critical to counter threats that are not only not confined to a single Field Division, but are not confined to a single country. In the wake of the September I 1, 2001 terrorist attacks, Director Mueller distributed new guidelines regarding case blocking. Per EC dated 10/03101 (66F-HQ-AI307721), cases cannot be restricted in ACS without the approval of the AD of the Criminal Investigative Division (CID), the AD of the National Security Division (NSD), or the AD of CTD. The EC emphasizes that, although blocking may be appropriate in some cases, Field Offices need to be able share critical information as efficiently as possible.
- Again, progress towards intelligence capacity is reported in the Director's Report on Counterterrorism.

Level 4 (Liaison Capacity): Responsibility for haison falls both within and without the CTD. Inside CTD, development and maintenance of key partnerships is prkiarily the responsibility of CrD Sections, therefore, accountability focuses on the Section Chiefs. Outside CTD, the CT Program is dependent on FBIHQ Support Divisions (e.g. OPCA, Finance, etc.) for maintenance of the external haison necessary for the success of the CTD Program Plans.

- Liaison issues and requirementstguidehnes for working with external partners are also addressed in the CTD Program Plans.

- The CTD equivalent of the SAC Phone Calls is the Section Chief (SC) Contracts. Like the Director's Report, this is a newly developed accountability mechanism which holds the SC accountable for progress towards maximum capacity. The SC of each of the four CTD Sections writes their own contract, which consists of priority actions that the SC will address over the next year, then meets with the AD for discussion. The priority actions are based on capacity assessments across Levels 1-4 and should represent the major gaps across their program that require immediate program management attention for resolution. Once the SC and AD have agreed on the priority actions to be included, the SC signs the contract. This contract will be reviewed by the AD at the end of the year to track progress by the Section, then will be used by the SC and AD as part of the continuing assessment process and as a basis for discussion on the new SC Contract.

Level 5 (Program Management Capacity): Due to the all-encompassing nature of the capacity covered in Level 5, all of the accountability mechanisms previously described contribute to **the** tracking of accountability for program management. **CTD Program Plans,** in **that** they represent the product (program strategy) of Level 5, are also accountability mechanisms for Level **5 to the** Deputy Director. Ultimate responsibility, however, lies with the AD, thus **this level** includes the use of another previously-established accountability mechanism, the AD Contract. This contract is updated every year and is agreed upon by the AD and the Deputy Director. The AD Contract is similar to the SC Contract, but the priority actions for the AD that require concerted executive management attention are drawn from the operational and management priorities defined through the Level 5 process. The AD Contract is written by the AD and discussed with the Deputy Director. The AD Contract provides yet another mechanism for assessment and accountability to the Deputy Director.

The multiple tools described above form a complex web of accountability that enables executive iganagement to match gaps and the strategies with the appropriate responsible party. These mechanisms allow CTI) to focus resources and effort where they are most needed and to track progress on closing capacity gaps. Since everyone in the program knows exactly what is expected of them, performance review .becomes a systematic and simple procedure. Continuous and multiple accountability mechanisms help move the program towards maximum feasible capacity more consistently.

Appendix D
Annual Field Office Report

Annual Field Office Report (AFOR)

Simultaneous to the initiation of MAXCAP05, the FBI was automating the AFOR. The AFOR, completed each year as the primary reporting document between the Field and FBIHQ, is a comprehensive document which contains everything from a detailed threat assessment to resource requests. Because the AFOR is so comprehensive, prior to its automation the information it contained was often not thoroughly reviewed and utilized at Headquarters. The Field paid less and less attention to the content they provided and thus, prior to automation, the AFOR had become a near futile exercise.

Beginning in 1999, the AFOR process was put entirely on-line. This meant that the Field could both review questions and enter data in a CD-ROM-based format which allowed for multiple simultaneous users. At FBIHQ, the program managers were not only able to review all of the field input on the FBI Intranet from their desks, but the database behind the AFOR made an endless combination of database reports available to HQ program managers, simplifying nationwide analysis.

While the AFOR remains a work-in-progress, the automation project was a huge success. In the summer of 2000, the CTT) ran its first fulscale review of the AFOR. Using the automated format, the CTD divided up the CT portions of the AFORs among CID HQ supervisors. Each HQ supervisor was asked to perform a thorough review of their assigned offices' AFORs and the resulting analysis was colited by the CTD Executive Staff for review by CTD executive managers. While this process was an enormous improvement over previous years, the 2000 APOR process still had two key gaps. First the questions the Field had been asked in the AFOR were out-dated and largely irrelevant, so the infoqtion which came in as a response was often times of little or no use. While these questions had been provided by CT managers, they were not coordinated with the criteria in the five levels. Second, while the AFOR responses came to the HQ supervisors in an automated format the review process at Headquarters remained heavily reliant on paper as SSAs passed their reviews up through their unit chiefs and section chiefs and summary ECs were sent to the Field. In 2001, CID and the FBI Office of Strategic Planning addressed both of these challenges.

In the winter of 2001, CTD completely reviewed and rewrote the questions asked in the CTD portion of the AFOR to reflect the FYO I criteria for Investigative Capacity (Level 1). In addition to rewriting the questions, the CTD added into the AFOR a requirement for capacity ratings. Each office was asked to report ratings in each of the five areas which make up Investigative Capacity, as well as ratings for their CT Program overall. This change proved to be a tremendous success. The Field found the questions much more relevant and easier to answer and HQ found the information much more digestible and helpful.

In addition to rewriting the CT portion of the AFOR in FYOI, the CfD, in conjunction with the FBI Office of Strategic Planning, initiated an effort to automate the HQ review piece of the AFOR process. The results of this project was an AFOR review site on the FBI Intranet where the HQ supervisors could not only review the AFORs of the offices they were assigned, but they could enter their conunents directly onto the site. The site also allowed for the review of the SSA's comments by Unit Chiefs and Section Chiefs directly onto the site, which significantly cut down on the required paperwork. Following the completed reviews, ECs back to the field were generated off the comment fields filled in at Headquarters and summary notebooks were prepared for CTD executive management using the database associated with the review site. Based on all of

these innovations, the FY01 AFOR cycle for the CT Program was a huge success and provided a comprehensive, in-depth, searchable, database of information describing the current level of 'mvestigative capacity. This information provided both the basis and the justification for the CTD FY03 budget request and a summary of the AFOR information was presented to FBI executive management via the Director's Report on Counterterrorism for use in policy development and internal resource allocation.

Director's Report on Counterterrorism

While the CTD has used many pre-existing tools to implement MAXCAP05 (the AFOR, Program Plans, SAC phone calls), the strategy did require a few new processes and products. One of these new products is the Director's Report on Counterterrorism. The centerpiece of the Director's Report, which is produced twice a year, is a summary of the current capacity in all five levels of the CT program. This information is provided in a number of different formats including color-coded maps, summary spreadsheets, and in-depth reviews of each field office. In addition, the Director's Report contains up-to-date information about major terrorist threats and lays out the AD's plan for countering those threats. The Director's Report is provided to the Director and Deputy Director. Program-sper-ific summaries are provided to each CT Section Chief and EC's summarizing the Report's findings are sent to the field.

The first Director's Report was published by CID on March 1, 2001. The Report was based primarily on the first field-wide assessment of Investigative Capacity completed in the winter of 2001. Ile second Direxor's Report was published September 1, 2001 following a complete review of the *FY01* AFOR which contained questions specific to CTD capacity The Director's Report has proved to be a valuable tool and has already been used both inside and outside the division to make policy decisions and develop resource requests.

The continuing challenge created by the development of the Director's Report is the issue of how widely it is distributed. Ilere are clear benefits to distributing the information on FBI CT capacity amongst our federal partners (DOJ, OMB, Congress) in order to facilitate partnerships focused on filling capacity gaps. There is, however, a clear down-side as well There is concern that [redacted] b7E On balance, the risks involved in broad dissemination of the Director's Report outweigh the benefits. To-date, therefore, distribution of the Report has remained limited to the FBI. The CTD planning staff does however make every effort to incorporate capacity information into aU reporting requirements to oversight agencies whenever possible. While capacity ratings themselves are not reported out, the **five** level strategy is incorporated into budget and performance measurement documents and the FBI has briefed external partners on MAXCAP05.

Appendix E
Staffing and Budgeting

From the beginning of the implementation phase of MAXCAP05 in March of 2000, staffing and budget questions have proved to be a formidable challenge. The challenges which came before the CRWG in these areas centered around three key issues:

1) Permanently staffing the MAXCAP05 initiative to ensure continuing progress and long-term integration into the Counterterrorism Program;

2) Streamlinffig the relationship between the CTD (an operational division) and the support divisions-,- most notably the newly formed Investigative Services Division; and

3) Integrating the assessments generated under MAXCAP05 into the CTD budget cycle in order to more clearly and specifically justify resource requests and allocations.

Staffing MAXCAP05

Because the heart of the MAXCAP05 initiative is intensive internal assessment, the CTWG realized early on that a permanent planning staff would be necessary. The CTWG understood that a small planning staff, reporting directly to the CTD AD would not only ensure the successful completion of the extensive workload requirements of MAXCAP05, but would also help to institutionalize the comniitment to integrated, national program management at the highest levels of the Division.

While consensus grew early-on about the need for a small planning staff. its implementation remains an outstanding issue. Since March of 2000, MAXCAP05 has continued to be staffed by an *ad hoc* group of original members of the CTWG. Impediments to the creation of a formahwd planning staff include an organizational bias against building new personnel structures which are non- operational in nature and a limited pool of internal personnel with the interests and academic disciplines required to successfully staff a unit responsible for planning.

CTD is actively addressing each of these issues with varied success. In the fall of 2001 for example, the CTD hired, through the Presidential Management Internship (PNU) Program, an analyst with a public administration background as well as previous experience with federal-level strategic planning initiatives. Additionally, a proposal outlining the parameters of the planning staff was approved in the early fall of 2001 and the work required to fill the new positions is underway.

CID and the Support Divisions

Prior to the formation of the CTD, the operational divisions at the FBI (the National Security Division and the Crininal Investigative Division) developed a mechanism for facilitating work with the FBI Service Divisions (Fhmce, IRB, IRD, OPCA, etc.)

which consisted of the establishment of "mini-support divisions' within the operational divisions. For "ample, despite the existence of the Fumce Division, the National Security Division (NSD) currently maintains a large budget unit who, among many other assignments, helps to formulate, fonnat, and execute the budget for NSD. This (ieoentmlization also existed in the arm of security, personnel, and computer support.

AD Watson saw the formulation of the new CTD as an opportunity to move away from this type of organization and towards a structure which relies mom heavily on the support divisions for critical infrastructure services, thus allowing the CTD to focus on national program management and operations. AD Watson's proposal included two parts. The first was the creation of an Executive Staff for CTD whose sole responsibility is to assess the inftastructure needs of the Division and work with the support divisions to ensure that those needs are being met. Second, the plan requires the creation of teams within each support division that specialize in counterterrorism. For example, in the area of security, AD Watson's model would have a vaember of the CTD Executive Staff whose responsibility it is to maintain liaison with the Security Countermeasures Section to ensure that CTD's needs are being met. In turn, the Countermeasures Section would designate a team to service CTD's specialized needs.

To date, the CTD has seen some success in improving its working arrangement with the service divisions. Internal to the CID, all objectives in this area have been met. AD Watson made good on his promise to not create a mini-headquarters within the Division and the CTD now has an Executive Staff which reports directly to the CT DAD through a Chief of Staff. In NIPC, there is a small Strategy and Planning Unit which coordinates support division needs for NIPC.

External to the Division, while there are not as yet Cr teams explicitly designated in each of the support divisions, progress has been made moving infrastructure work formerly done within the operational divisions back out to the service divisions. All computer support services have been moved back to IRD and all personnel services have been moved back to ASD.

The next functions to be addressed are financial and budgetary. The success in limiting the creation of internal service staff in CTD is due in large part to the wiftgncss of the NSD budget staff to continue to coordinate Cr related taskings while CM develops new working arrangements with support divisions. While NSD's help in this area has provided a crucial bridge, CM recognizes that it is not a long-term solution. FD already has staff fanutiar with the CT Program and NSD budget staff and FD budget staff already work well together, so the planned re-centrahzation of budget functions and the creation of specialized CT teams within FD should improve the incorporation of MAXCAP05 into the budget process.

The Budget Cycle

The CT Program will never reach in ' aximum feasible capacity without sufficient resources strategically placed. Full integration of the assessments generated under MAXCAP05 into the budget cycle is, therefore, a critical piece of implementing the strategy. The consistency produced by systematic assessment makes the budget process easier and better connected to the CT program's strategy.

CTD has already achieved quite a bit of success in its effort to foid the MAXCAP05 assessment results into the budget process. In the spring of 2001, the formulation of the FY03 budget was, for the first time, based entirely on MAXCAP05

assessments in all five levels of the strategy. Additionally, since the first complete assessment in March of 2001, all management decisions regarding resource allocation have been informed by MAXCAP05 assessment results. Further, since the first automated assessments were completed in the summer of 2001 through the FY02 AFOR, information necessary for resource allocation has been increasingly utihwd by executive management due to its improved accessibility.

While CTD has bad success integrating MAXCAP05 into the budget cycle to better inform resource requests and allocations, several challenges remain. Paramount among the budget challenges for CTD is the nature of the federal budget cycle, which requires agencies to project their budget needs two to three years into the future. While MAXCAP05 assessment tools are extensive, they do not currently require the program to do the same kind of long-run projections required in the budget process.

Additionally, fully integrating MAXCAP05 data into the budget process has been hampered by staffing challenges. As previously discussed, budgeting functions are decentralized in FD and NSD and CTD plans to work FD to re-centralize these functions, which should improve the incorporation of MAXCAP05 into the budget process. The roles of the CTD Executive Staff and the proposed planning staff also need to be defined as this re-centralization proceeds, so that CTD's priorities and strategies are My and effectively incorporated into the budget and communicated externally.

Appendix F
Minding the Gaps

The CTD has had great success in redirecting the national CT Program away from a case-driven, reactive management style and towards a more effective management approach which focuses on achieving maximum feasible capacity. The CTD has achieved this success by instituting intensive assessment tools and applying the required resources toward analyzing the assessment results. Now that a system for ongoing, meaningful assessment has been put in place, the CT Program is in the process of focusing its resources on closing the gaps in capacity which have been uncovered at every level of the program.

Prioritizing these next steps towards achieving maximum feasible capacity is critical. Not only will clear priorities help focus CM's efforts, but it will also allow CTD to articulate to its partners, both inside and outside the FBI, the areas in which the CT program needs priority assistance. Next steps are most easily understood and put into action when they are divided

into three categories: systemic, organizational, and operational.

Systemic Gaps

Before the CTD began implementation of MAXCAP05, CT managers in the Field at FBIHQ and analysis constituted the most significant gaps in the CT Program. While these gaps have been discussed and communicated to external entities (DOJ, OMB, Congress, etc.) through the budget and other external reporting requirements, MAXCAP05 has allowed the CTD to better document the situation. Information gathered through the AFOR and articulated in the Director's Report systematically confimls that training, translation, and analysis are the critical gaps that require immediate attention. The events of September 11, 2001 underscore these critical needs. The CTD, therefore, has a number of initiatives underway in each of these areas to work towards maximum feasible capacity in these three areas.

Training

Counterterrorism:

The New Agents curriculum has been revised to incorporate more counterintelligence (CI) and CT training. The block of time allocated to DT has been increased and a DT practical problem has been included. The IT section is still inadequate, but discussion is underway to increase the IT time and to include an IT practical problem based on Charlotte Division's recent Hizballah case.

- CTD is working with the Leadership and Management Science Unit, CID, and NSD's Operational Training Unit (OTU) on FBIHQ Supervisory Special Agent In-Services.
- The Professional Development Unit hosted a meeting of the Strategic Planning Curriculum Working Group from 09119/01-09/20/01. This group was formed to develop and coordinate strategic planning training throughout the Bureau and is coordinated with the Office of Strategic Planning. Several members of the group attended performance measurement training.in November 2001.

International Training

- The IT Interactive Multimedia Instruction and Simulation (IMIS) Program Distance Learning CDROM has been finished and approximately 40 Special Agents have completed the course. An additional 1,000 CDs are ready to be sent to each Field Office and Resident Agency. OTU also has CD-ROM drives in stock which they will distribute to the field as needed. This distance Learning course serves as a continuing education credit and a prerequisite for the Basic International Terrorism Operations In-Service.

- The agenda for the Basic IT Operations In-Service is almost finalized and the course can be taught on very short notice. Instructors for the course are drawn from FBI, DOJ, [redacted] DOS, [redacted] and INS. Th-s course also serves as a continuing education credit and is required for promotion to GS-13. Basic in-services are planned back-to-back to train as many agents as possible in the least amount of time. b7E

- Preliminary agendas for Intermediate and Advanced IT hi-Services are under review. These courses will include [redacted] and will address IT program priorities and strategies, interaction with other domestic and foreign services, area studies and cultural awareness, terrorist fund-raising and money laundering activities, sensitive b7E

investigative techniques, case management, and strategic planning.

- OTU and CM are looking into utilizing a course developed by a retired Special Agent and [redacted] called Intelligence and Law Enforcement: Attacking Transnational Targets. The course is interactive, class size is limited, and after a recent test at the FBI Academy, received good reviews from participants. OTU and CTD have met with the relevant contacts, and received a commitment to revise the course to target the IT program and provide a tentative schedule for training. This course could be taught regionally, in any location with secure facilities. b7E

- The Center for Counterintelligence and Security Awareness is a private company run by two retired Special Agents and specializes in counterintelligence awareness training. They have undertaken a CT training mission and have approached the FBI about providing training to FBI personnel. Instructors are drawn from retired Special Agents and intelligence officers and the courses could be taught regionally or at Quantico with minimal strain on FBI operational personnel.

- OTU and CTD agree that all **National Foreign Intelligence Program** (NFEPI) **courses** should have blended content that is relevant to both the CI and CT Programs. OTU has agreed that IT will be emphasized and that half of the slots for each NFIP In-Service will be reserved for the CT Program.

Domestic Terrorism:

- The DT IMIS Distance Learning CD-ROM is finished and awaits minor edits before being sent out to the field.
- DT/CPS has a basic operations course already, so OTU and DT/CPS will coordinate on a Basic DT Operations In-Service. DT may be able to turn the Basic In-Service over to OTU and focus on intermediate and advanced courses.

Translation

Translation has been an issue since the beginning of the CTD planning initiative and discussions have included faster clearance times for applicants and the possible creation of a Language Center to centralize t, Aviation capabilities. After the September 11 attacks, the Director issued a request to the public translators and the Bureau has received many applications. Currently, translators are working through [redacted] background investigations on translator applications have been prioritized and streamlined, and discussions continue about moving translation capabilities to an off-site location. Involving the FBIs translation capacity is one of the Director's highest priorities. b7E

Analysis

The CTD has proposed an intelligence pilot to address the gaps in the CT Programs intelligence and analysis capabilities. This effort differs from traditional intelligence methodology in two ways:

- This pilot is aimed at identifying previously unknown activities and intentions of terrorists, instead of just reorganizing and repackaging known information.
- This pilot recognizes that only those responsible for the CT program and its investigations have the expertise and

experience to determine intelligence requirements, apply the information, and evaluate its effectiveness. The intelligence effort must be driven by the investigators.

Cooperation with ISD is critical to the success of this initiative in the coordination of collection and dissemination requirements, maintenance of data bases, and the development of analytical approaches and products and strategic cross-cutting analyses. CTD and ISD will work together to focus on the CT Program's top investigative objectives, identify systemic critical intelligence gaps and shortfalls, focus on providing new information, and produce a range of intelligence products.

This pilot project has five phases. Prior to beginning Phase 1, subject matter specific CTD Intelligence Working Groups (IWG) will be established (e.g. HAMAS, UBL, ALF/ELF, etc.). The members of the working group will have specific knowledge of and experience working on the target groups and will facilitate communication between the CTD, ISD, and the field. Each IWG will consist of.

2-3 subject matter experts from the field;
1-2 subject matter experts from CID;
ISD representatives); and
One CTD manager to oversee the group's progress.

Each CTD Section with responsibility for PIRs will make at least one analyst available full-time: for the pilot. One CTD manager will be selected to coordinate the efforts of all the IWGs, to monitor the direction and operation of the project, and to revise the project as necessary.

Phase 1: Identification of priority intelligence requirements (P[Rs)

Working with program managers and case agents, each IWG will determine critical information requirements for the specific target group. This phase will produce a list of strategic, operational, and tactical PIRs that will form the basis for the project. These PIRs will be reviewed bi-weekly by the IWG to ensure continued relevance.

Phase 2: Analysis of available information

AU available information will be reviewed and analyzed in support of the PIRs developed in Phase 1. This phase includes bA searches of FBI systems, a review of recently completed AFORS, a review of federal law enforcement and intelligence agencies data, analysis of state and local police records, and a review of available foreign source information. Phase 2 will also include the use of high quality analytical tools to facilitate linkage analysis and behavioral pattern analysis. Any information not conclusively addressed in this Phase 2 process will be identified as intelligence gaps, which in turn constitute new collection requirements.

Phase 3: Collection of information needed to close intelligence gaps

The collection requirements identified in Phase 2 will be forwarded to ISD, which will then issue the new requirements to Field Offices, Legat Offices, and other relevant agencies in an effort to close the information gaps.

ISD will receive data, analyze it, and systematically report both data and analysis to CTD on a regular basis. During this process, ISD will both confirm old information as well as identify [redacted] b7E

[redacted]

Phase 4: Reporting and integration into investigations

AD information collected by ISD will be forwarded to the IWGs, which will then conduct a comprehensive analysis and will prepare intelligence products designed to enhance investigative programs. These intelligence reports will provide information on key aspects of the investigation, including but not limited to:

- [redacted] b7E

These reports will be reviewed for new information requirements (IRs). This phase will be characterized by a long-term flow of information to and from collectors. analysts, and investigators. Pilot team members will be responsible for ensuring that intelligence analyses are integrated into investigations through close work with case agents and full information sharing.

Phase 5: Conclusions, evaluations, and integration

Under this phase, CTD will conduct a thorough, impartial assessment of the substance of the intelligence and the processes employed. Through contacts with Field Offices receiving intelligence, the CM will determine the extent to which the information enhanced investigations and will recommend adjustments to the process as necessary. This effort will be continually evaluated by CID Executive Management to ensure effectiveness.

Given the critical nature of the CT Programs, intelligence gaps, this pilot is intended to last no more than 120 days, with reporting and evaluation conducted every 30 days. At the end of the project, CID and ISD will develop a plan for broader implementation based on lessons learned through the pilot.

Organizational Gaps

As this workbook has brought to light, there are also a number of organizational gaps which need to be addressed in order to achieve maximum capacity, including:

1. 1. Implementation of Trilogy: IRD's information infrastructure upgrade will significantly enhance the capacity of CTD by facilitating information flow and communication, both inside and outside the Bureau. Throughout Trilogy development and implementation, CTD will stay informed regarding additional or altered capabilities efficiently and effectively. CTD, in conjunction with IRD, will keep the Field fully informed of Trilogy developments so the Agents and Analysts can quickly integrate new information technology systems and functions into investigations and analyses. CTD will also maintain constant communication with IRD regarding training for Agents and Analysts on new or altered systems.

2. Planning Staff- While substantial work continues on MAXCAP05, the *ad hoc* nature of the planning staff presents a barrier to full implementation and institutionali7Ation of the initiative.neproposed planning staff constitutes a critical bridge between the decisions of CTD Executive Management and the CTWG and the actual implementation and maintenance of MAXCAP05 systems and processes.

3. Executive Staff. Fully staffing the Executive Staff is necessary to facilitate the re-consolidation of support functions and ensure smooth working relationsmps with service divisions, allowing investigators and analysts to focus on operational concerns with the support they need to most effectively do their jobs.

4. Performance Measurement Reporting: CTD needs to address performance measurement mechanisms to report progress to external entities and the American public. The CT Program has struggled to find ways to report progress without riskin misinterpretation of capacity ratings, but with the current renewed focus on counterterrorism, the FBI needs to find a way to report to the Congress and the American people about the CT Program's progress in pursuing maximum feasible capacity. This issue will be one of the first priorities of the proposed CTD planning staff.

Operational Gaps

In terms of operational next steps, the CID executive level meetings in FY01 (as required by Level 5) produced Program Plans for each of the four CT programs which outline operational priorities. The following is a summary of the operational priorities as outlined in the CM's FY02 Program Plans for IT, DT, NIPC, and NDPO.

CTD Plans roll- up, operational priorities and strategies

Counterterrorism Division
International Terrorism Program

Strategic Program Plan
FY 2001-2006

Mission:
The International Terrorism Program's mission is to: identify, prevent, and deter the activities of international terrorists prior to the commission of a terrorist act and to pursue the arrest and prosecution of international terrorists who have conducted or aided and abetted those engaged in criminal acts of terrorism.

Strategic Assessment:

(U) (S) The vast network of international terrorist activity targeted against United States (U.S.) interests is significant, and credible threats are emerging with increasing frequency. **The international terrorist threat can be divided into three categories: radical international jihad movement, State Sponsors of terrorism, and formalized terrorist groups.** State Sponsors and formalized terrorist groups present significant challenges, but they represent threats that are generally known to U.S. law enforcement and intelligence communities. The FBI, therefore, has a relatively solid target on which to focus pro-active efforts against these threats. Threats from the radical international jihad movement, however, challenge the FBI to conduct pro-active investigation into the activities of countries, groups, and individuals which have not previously been the subject of investigative attention and about which both the FBI and the rest of the Counterterrorism Community have limited but growing knowledge or expertise. The threat is more difficult to identify, is more likely to be based on indirect U.S. involvement overseas, and is more likely to be channeled through one-time collaborators, lone offenders, or groups on which the U.S. has no data or expertise.

(U) (S) The FBI believes that the threat posed by international terrorists in each of these three categories will continue for the foreseeable future. A trend in international terrorism that the FBI has seen develop in recent years is the execution of high intensity, indiscriminate, mass casualty attacks. The FBI projects the continuation of this trend in future years, with attacks particularly perpetrated by radical international jihad extremists. These extremists have built networks, in the U.S. and abroad,

which provide the infrastructure through which supporters of terrorism maintain contact with each other and with like-minded individuals internationally. The extremists have developed a global connection of supporters and operatives whose common enemies are the West and the Middle Eastern governments who do not support an Islamic extremist agenda.

Radical International Jihad Movement

(U) ~~(S)~~ The most serious international terrorist threat to U.S. interests today stems from Sunni Islamic extremists, such as Bin Ladin and individuals affiliated with Al Qaida who are supporters of the Radical International Jihad Movement. Al Qaida is a vast, well financed, criminal organization comprised of structured, hierarchical cells. Al Qaida's willingness and capability to inflict large scale violence and destruction against U.S. persons and interests as they did in the East African bombings make them a clear and imminent threat to the U.S. However, the threat from Al Qaida is only a part of the overall threat from the Radical International Jihad Movement which is composed of individuals of varying nationality, ethnicity, tribe, race, and terrorist group membership who consistently work together in support of Sunni terrorism goals. The single common element among these diverse individuals is their commitment to the radical International Jihad Movement, which includes a radicalized ideology and agenda promoting the use of violence against the "enemies of Islam" in order to overthrow all governments which are not ruled by Sharia law. A primary objective of this movement is the successful planning and implementation of large scale terrorist events against U.S. interests and citizens, maximizing casualties.

(U) ~~(S)~~ Currently, one of the most recognized proponents of the International Jihad Movement is Usama Bin Ladin. His arrest and prosecution has become one of the highest priorities of the FBI. Since 1996, Usama Bin Ladin has made numerous threats against U.S. interest including his August 22, 1996 declaration of Jihad (Holy War) against the U.S. Specifically, Bin Ladin is believed to be connected with multiple terrorist incidents around the world including the World Trade Center bombing and the bombings of the American Embassies in Kenya and Tanzania in August of 1998. All of these operations relied on multinational, multiethnic, multiracial participants who shared a devotion to a radicalized agenda.

(U) ~~(S)~~ More recently, during December of 1999 and January of 2000, the International Terrorism (IT) Program's time and focus were occupied by the combined events associated with the Millennium, as well as the intensive investigation which followed the arrest of Ahmed Ressam, an Algerian extremist associated with the Armed Islamic Group (GIA), at the U.S.-Canadian border crossing on December 14, 1999 (BORDERBOM).

Investigation to date reveals that Bin Ladin's ties to BORDERBOM are indirect as would be expected among any confederation of individuals who share training facilities, financing, or logistical assistance.

(U) ~~(S)~~ The recent Jordanian Millenmnium threat and BORDERBOM conspiracies are examples of this expanding International Jihad Movement. [redacted] b7E

State Sponsors

(U) (S) The U.S. Department of State has designated seven countries as State Sponsors of terrorism. They are Iran, Iraq, Syria, Sudan, Libya, Cuba, and North Korea. In recent years, the terrorist activities of Cuba and North Korea have declined as their economies have deteriorated. However, the activities of the other State Sponsors have continued, and in some cases, have intensified during the past several years.

Iran

(S) b1 b3

(S) b1 b3

(S) b1 b3

(S) b1 b3

Iraq

(S) b1 b3

(S) b1 b3

(S)

b1
b3

(S)

b1
b3

(S)

b1
b3

(S)

b1
b3

Syria

(S)

b1
b3

(S) [redacted] b1 b3

[redacted] b1 b3

(S)

Libya

(U) ~~(S)~~ The Government of Libya (GOL) continues to be considered terrorist threat. Although the GOL has been a significant sponsor of terrorism during the last few decades under the leadership of Mu'ammar Qadhafi, the GOL is currently trying to be accepted back into the "community of nations" by turning over the two suspects in the December 21, 1988, bombing of Pan Am 103 which killed 270 people including 189 Americans.

(S) [redacted] b1 b3

[redacted] b1 b3

(S)

Sudan

[redacted] b1 b3

(S)

(S) [redacted] b1 b3

(S) [redacted] b1 b3

(S) [redacted] b1 b3

Formalized Terrorist Groups

(U) (S) Formalized terrorist groups are autonomous organizations that have their own infrastructures, personnel, financial arrangements, and training facilities. They are able to plan and mount terrorist campaigns overseas, as well as support terrorist operations within the U.S.

(S) [redacted] b1 b3

(S) [redacted] b1 b3

(S) [redacted] b1 b3

(S) [redacted] b1 b3

(U) (S) The Egyptian Al-Gama'a Al-Islamiyya, or Islamic Group (IG) is an International Radical Fundamentalist (IRF) group based in Egypt. Its principal objective is to overthrow the secular oriented government of Egypt and replace it with an Islamic based authority. The spiritual leader of the group, Sheikh Omar Ahmed Ali Abdel Rahman, is currently incarcerated in Rochester, Minnesota, for his involvement in the 1993 conspiracy to bomb several major New York City landmarks. In February 1998, a leader of the IG, signed a fatwa (religious decree) issued by international terrorist financier, Usama Bin Ladin which called for the killing of American citizens. The threat has been repeated following published reports of rough treatment of Sheikh Rahman by U.S. prison officials.

(S) [redacted] b1 b3

(U) (S) Recent security crackdowns by the Government of Egypt (GOE), together with the IG fractionalization within its leadership have damaged the IG's network. However, the IG still retains a formidable terrorist capability.

The United States' support of GOE initiatives to render IG, Egyptian nationals to Cairo for trial has drawn significant criticism from the IG and may serve as a justification for future attacks against American citizens and interests overseas. Furthermore, as long as Sheikh Rahman remains in U.S. custody, the U.S. will continue to serve as a potential target for lethal IG activities.

(U) (S) Like the IG, the Egyptian Islamic Jihad (EIJ) is also an IRF group whose principal objective is to overthrow the secular oriented GOE and replace it with a system based on Islamic law. The EIJ is smaller than the IG, but has distinguished itself by aligning closely with members of Saudi terrorist financier Usama Bin Ladin's group, Al Qaeda. In February 1998, Aiman Zawahiri, a leader of the EIJ, also signed the fatwa issued by Bin Ladin. The EIJ echos threats made by the IG against the U.S. for its detention of the EIJ's spiritual leader, Sheikh Rahman.

(U) (S) The EIJ is widely credited with the November 17, 1995, bombing of the Egyptian embassy in Islamabad, Pakistan and has a demonstrated capability to act outside of Egypt.

(S) [redacted] b1 b3

(U) (S) In February 1999, the Government of Albania rendered several suspected Egyptian extremists to Egypt for trial. Continued U.S. support of GOE initiatives to render EIJ members to Egypt for trial has drawn significant criticism from the EIJ, and may serve as

justification for future attacks against American citizens and interests overseas. Although continued security crackdowns by the GOE have damaged the EIJ's network, the EIJ's tacit alliance with Bin Ladin is an additional cause for U.S. concern since Bin Ladin remains firmly committed to disrupting U.S. interests worldwide.

(S) (U) (S) [redacted] HAMAS members engage in various activities in the U.S. through two front organizations (the Holy Land Foundation for Relief and Development and the Islamic Association for Palestine). HAMAS is an Islamic fundamentalist terrorist organization dedicated to establishing a Palestinian state from the Jordan River to the Mediterranean Sea. HAMAS was designated as an international terrorist organization by the U.S. Secretary of State on October 8, 1997, pursuant to the Anti-Terrorism and Effective Death Penalty Act of 1996. HAMAS rejects Yasir Arafat as the leader of the Palestinian people and opposes the Israeli-PLO Declaration of Principles that gives the Palestine Authority control of Gaza and portions of the West Bank. HAMAS terrorist actions have directly impacted U.S. interests and has caused the deaths and injury of U.S. citizens.

b1
b3

Performance Gap

(U) (S) Over the past two years, the IT Program has been enormously successful in positioning its resources to provide an effective deterrent to international terrorism and the activities of State Sponsors. The successes of the past, however, are in large part the result of the extraordinary dedication of the FBI Agents and professional support personnel assigned to the program, and should not be taken for granted. The precise capabilities of terrorist groups and the capabilities of State Sponsors to gather intelligence to inflict harm to American interests, and the full scope of the network in which they and their allies operate, is not yet fully understood.

(U) (S) The CTD has made a firm commitment to enhance national IT Program strategy, planning, and coordination. During July and August of 2000, at four regional conferences, CTD presented to all the FBI's field Assistant Directors in Charge (ADIC) and Special Agents in Charge (SAC) the new, nationally-directed, five level program management strategy to bolster field, headquarters, and interagency capacity to fight terrorism. The importance of this effort was underscored by the changing nature and scope of terrorist threats and the FBI's designation of the CT Program as a "Tier 1" national priority.

The field executives made it abundantly clear that the major obstacles preventing them achieving maximum capacity in their IT Programs were the critical lack of trained intelligence analysts, translation capability, and IT related training for their Agents working in the IT Program.

(U) (S) These obstacles are within the ability of the FBI to address. The Investigative Services Division must make it a top priority to: hire capable analysts with the appropriate education and background; train the new analysts as well as the current analysts assigned to the IT Program; and address the critical need for translators. The Training Division must reorient its priorities to the Tier structure and immediately provide for basic, intermediate and advanced IT training for field Agents. Without the full and complete support of these divisions, the IT Program will continue to have recognized performance gaps which result in an unacceptable vulnerability in a Tier 1 program.

Five-Year Program Goals

- **Identify, Prevent and Deter International Terrorist Operations**
- **Identify, Prevent and Deter** Foreign Intelligence Operations

Investigate and Bring to Justice International Terrorists Who Have Conducted or Aided and Abetted Those Engaged in Acts of International Terrorism.

Strategy

(U) Approaching the most technologically advanced and globally connected era in the world's history, there is no greater or more meaningful challenge than the opportunity to bolster FBI capability to counter international terrorist threats in the physical and cyber arenas. The Counterterrorism Division (CTD) has made a firm commitment to enhancing national counterterrorism program management and has initiated a new, nationally-directed five level program management strategy to bolster field, headquarters, and interagency capacity to fight terrorism. The importance of this effort is underscored by the changing nature and scope of terrorist threats and the FBI's designation of the IT Program as a "Tier 1" priority.

The Five Level Strategy:

(U) The Counterterrorism Division defines maximum feasible capacity in terms of five principal categories or levels. This five level strategy serves a framework for ensuring that the IT Program is doing everything within its power to counter terrorist threats and serves as a blueprint for interagency coordination and long range planning efforts to reduce vulnerabilities and build capacity for investigative and emergency response. Each of the five levels represent integral components of the IT Program which must function together for optimal performance. These levels are outlined as follows:

FIVE LEVEL STRATEGY (U)	
Level 1: Field Capacity	The extent to which each FBI Field Office is appropriately staffed, trained, equipped, and managed to prevent and effectively respond to acts of terrorism.
Level 2: Headquarters Capacity	The extent to which FBI Headquarters can provide value and support to field investigations and can provide nationally-coordinated program management.

Level 3: FBI Capacity	The pro-active capability to fully utilize and integrate FBI resources throughout the FBI in support of IT programs and initiatives.
Level 4: Interagency Liaison Capacity	The establishment and maintenance of sound and productive relationships with external counterparts in the intelligence community, law enforcement communities, other federal agencies, defense establishments, foreign services, private industry and non-governmental organizations, state and local agencies, legislative and executive bodies, the media, and academia to obtain maximum information and support.
Level 5: Complex Operations Capacity	The capacity to use all necessary assets and capabilities to support and initiate complex operations designed to penetrate and neutralize international terrorist threats.

Criteria:

(U) Each of the five levels includes specific evaluative criteria pertaining to the IT Program. These criteria identify the specific program elements which must be present for the program to be at maximum capacity. These criteria will be re-evaluated and updated annually through the IT Program plan to reflect new initiatives, changing priorities, and to track progress toward reducing major vulnerabilities.

Capacity Ratings:

(U) To evaluate and improve program capability and performance in each of the five levels, the CTD has developed a summary rating system to track program criteria, identify performance gaps, focus management attention on resource deficiencies, and take actions to address vulnerabilities. To allow executive management to see progress towards maximum feasible capacity at a glance, the CTD has developed a color based rating system that evaluates overall capability in terms of three major categories; **Green** denotes maximum feasible capacity, **Yellow** denotes vulnerable, but making progress, and **Red** means vulnerable with significant problems continuing. For each of the five levels, the responsible official will conduct an self-assessment and rate their program using this color-based system. ADIC/SACs will evaluate their own field office IT Programs with this system based on the criteria for Level 1 (Field Capacity), while the Assistant Director of CTD will conduct an overall assessment of Field Capacity as well as assessing the capacity of the IT Program in Levels 2 - 5.

(U) This performance measurement system will provide a complete, national depiction of the IT Program from the field, headquarters, and interagency perspectives.
While there is a degree of subjectivity involved, these documented criteria and selective performance measures will provide both a clear blueprint of where program capabilities are strong and identify vulnerabilities requiring management's attention and resources.

Once all the criteria have been evaluated, and capacity ratings have been assigned to each field division and Headquarters Level, the IT Program will have a powerful information resource with which to make strategic policy and resource decisions and to correct vulnerabilities and develop safeguards. This information will be compiled for inclusion in the new Director's Report on Counterterrorism which will provide an assessment of the primary terrorist threats and vulnerabilities facing the nation and a snapshot of the IT Program capability in each field office and at Headquarters.

(U) The success of this new national program management strategy ultimately depends upon accurate and detailed reporting of vulnerabilities so that management's attention and resources can be devoted accordingly. While recognizing that the FBI will not be able to prevent all terrorist acts due to external factors, the most powerful defenses we have available are information and preparation. The Assistant Director of CTD and all the ADIC/SACs will pro-actively use this evaluation tool to assess current capability, identify performance gaps, and develop strategies to bring the Field Divisions to maximum feasible capacity. Accountability for both field and Headquarters program management in the IT Program will be achieved through the Director's Report on Counterterrorism, the inspection process, and ultimately through the performance appraisal system.

Dependencies, Obstacles, Mitigating Factors

(U) ~~(S)~~ Coordinating a worldwide program to counter the terrorist threat and to target State Sponsors requires the resources necessary to collect and exploit intelligence, and to develop appropriate technology needed to support the worldwide communication of vital information. Currently, Field and FBIHQ staffing in the IT Program is inadequate. Nearly every field office as well as the ITOS needs additional Agent and Analytical personnel. The field alone requested 91 more Agent positions than were allocated for the IT program in FY 2001. Further, many offices as well as the ITOS have reported that their operational travel funds are significantly inadequate and that investigations are being adversely impacted as a result.

(U) ~~(S)~~ Additionally, the FBI's current information technology system does not meet the IT Program's need to share information internally and disseminate information externally. This is particularly true in the case of sharing criminal and intelligence information among users. Taken together, these resource problems constitute a significant constraint on the IT Program and have heightened U.S. vulnerability to a terrorist incident and the efforts of State Sponsors.

(U) ~~(S)~~ In developing a strategic response to the terrorist threat, the IT Program's challenge is to organize its available resources and to develop an agenda for action that takes advantage of the FBI's unique capacity. The new CTD Five Level Strategy proceeds from

four assumptions:

1) The political/religious/social movements which drive terrorist acts are beyond the control of the FBI's counter-terrorism program. Therefore, the FBI will never be able to prevent all acts of terrorism against U.S. interests; 2) Acts of terrorism will continue to be regarded as the preeminent threat to U.S. national security interests; 3) The FBI will maintain appropriate staffing and funding levels over the next five years, and; 4) The IT Program will continue to oversee and coordinate all aspects of the FBI 's Counterterrorism Strategy during this period.

Critical Success Factors

(U) ~~(S)~~ ***CSF 1: Field Capacity: The extent to which each FBI field office is appropriately staffed, trained, equipped, and managed to prevent and effectively respond to acts of terrorism. In order for the field office to be at maximum capacity, they must have fulfilled requirements in each of the following field categories: Base of Knowledge; Understanding of Local Environment; Analytical Capabilities; Communication Capacity; and Disruption/Offensive Initiatives.***

FY01 Priority Actions

- Field Offices will make staffing decisions relating to IT squads which reflect the Tier 1 nature of the IT program.
- Field Offices will ensure that all personnel on their Office's IT squad have attended all available IT related training appropriate to their experience level.
- Field Offices will establish written protocols for verifying, approving, and disseminating annual IT threat assessments for their Division through the Annual Field Office Report.
- Field Offices will focus analytical resources on providing tactical analytical services to the IT program.
- Field Offices will establish and enforce a policy of maximizing information sharing with all appropriate FBI entities (within legal parameters) through the uploading and unblocking of IT case-related information.
- Field Offices will have a Joint Terrorism Task Force or a formal Counterterrorism Working Group capable of addressing international terrorism matters.
- Field Offices will establish protocols to ensure [redacted] b7E
- Field Offices will ensure that IT issues are regularly addressed through existing relationships with international, national,

state and local partners.

- Field Offices will ensure their Office's participation in all relevant IT exercises

- Field Offices will ensure that their Office's IT investigations focus on the development of human sources and the criminal prosecution of known terrorists.

(U) ~~(S)~~ ***CSF-2: FBI Headquarters Capacity: The extent to which FBI Headquarters can provide value and support to field investigations and can provide nationally-coordinated program management. In order for the IT Program be at maximum capacity, it must have fulfilled requirements in each of the following HQ categories: Base of Knowledge; Communication and Information Flow; Analytical Capability; and Response and Direction to the Field.***

FY01 Priority Actions

- The ITOS will articulate and encourage the application of IT program priorities in the Field.

- The ITOS will develop an IT threat assessment protocol for use by the Field.

- The ITOS will ensure that its personnel have attended all available IT related training appropriate to their experience level.

- The ITOS will develop the capability to extract pertinent, non-operational specific tasking from operational units.

- The ITOS will implement the "notes protocol" for sharing information between ITOS units.

- The ITOS will develop an IT operational manual for use by both the Field and HQ personnel and ensure the timely and accurate updating of the Fugitive Handbook.

- The ITOS will pursue a tactical, analytical capacity for each ITOS operational unit.

- The ITOS will issue daily threat reporting to the Field as well communications updating the IT Program's status.

- The ITOS will dedicate management resources to the strategic planning process.

(U) ~~(S)~~ ***CSF-3: FBI Capacity: A pro-active capability to fully utilize and integrate IT Program resources throughout the Bureau in support of IT programs and initiatives. In order for the IT Program to be at maximum capacity, it must fulfill requirements in each of the following bureau-wide categories: Assess; Articulate; Integrate; and Evaluate.***

FY01 Priority Actions

- The ITOS will develop a method by which to accurately, and consistently, articulate the IT Program's fiscal needs and priorities to the Finance Division.

- The ITOS will assess the IT training opportunities which are currently available, including the IT curriculum in the New Agents' Training Program at the FBI Academy, and provide the assessment and recommendations to the Training Division.

- The ITOS will assess the IT Program's needs vis-à-vis Investigative Services Division (ISD) (specifically: the development and regular dissemination of strategic and tactical analytical products to the Field; the tactical analytical support to the ITOS, and the management and operations of SIOC), and present a proposed protocol for addressing those needs to ISD.

- The ITOS will assess ITOS' facilities needs (specifically, conference room and office space issues) and articulate those needs and recommendations to the Administrative Services Division (ASD).

- The ITOS will assess the needs of the IT Program concerning the development of additional LEGAT offices overseas, and for present those findings and recommendations to ISD.

- The ITOS will participate in monthly meetings of appropriate Assistant Directors to discuss IT Program needs and priorities.

(U) ~~(S)~~ ***CSF-4: Interagency Liaison Capacity: Use the establishment and maintenance of sound and productive relationships with external counterparts in the intelligence community, law enforcement communities, other federal agencies, defense establishment, foreign services, private industry and non-governmental organizations, state and local agencies, legislative and executive bodies, the media, and academia, to obtain maximum information and support. In order for the IT Program to be at maximum capacity, it must fulfill requirements in each of the following operations management catagories: Identify Partners; Establish Relationships; Mutual Needs Assessments; Information Sharing; and Capability for Joint Product Development When Necessary.***

FY01 Priority Actions

- In conjunction with the Field, the ITOS will prioritize current relationships with federal, state and local agencies as well as foreign services and restructure the IT Program's method of fulfilling inter-agency requests to reflect those priorities.

- The ITOS will develop a program for briefing all out-going Ambassadors, Deputy Chiefs of Mission (DCM), Chiefs of Station (COS), and Deputy Chiefs of Station (DCOS) on ITOS program priorities and for briefing these executives at their annual meetings.

- The ITOS will assess and articulate ITOS' interest in and need for the Attorney General's proposed "War Room/Translation Center".

- The ITOS will maintain close and productive relationships with critical partners in order to ensure the continuing success of ITOS' personnel exchange program..

- The ITOS will ensure the IT Program's continuing participation in the FEST program and all related exercises.

- The ITOS will continue to represent the FBI's IT Program's interests on the Counterterrorism Security Group (CSG).

(U) ~~(S)~~ ***CSF-5: The capacity to use all necessary assets and capabilities to support and initiate complex operations designed to penetrate and neutralize terrorist threat. In order for the IT Program to be at maximum capacity, they must fulfill requirements in each of the following pro-active categories: Command and Control Infrastructure at HQ and the Field; Emergency Interagency Coordination Mechanisms; and Crisis-based Resources.***

FY01 Priority Actions

- The ITOS will develop a SIOC organizational structure for all IT-interagency "specials" and document a protocol for those situations.

- The ITOS will develop an interagency system to develop and vet complex investigative initiatives such as terrorist fund raising investigations.

PERFORMANCE MEASURES

(U) Central to the challenge of meaningful performance measurement for law enforcement is the problem of measuring deterrence. Each of the Five Levels has been broken down into discrete criteria that must be met for the IT Program to be at maximum feasible capacity. These criteria become performance measures through which the IT Program can be evaluated. Criteria and performance measures will be re-evaluated and updated annually through the IT Strategic Program Plan to reflect progress, new initiatives, and changing priorities.

(U) Tracking these criteria will allow the IT Program to identify performance gaps, to focus management attention on these gaps, to strategically allocate resources to address these gaps, and to formulate program budget requests. For example, if the application of the criteria indicates a gap in analytical capability across the field and at FBI Headquarters, the IT Program's management will then pro-actively focus existing resources more effectively towards bolstering analytical capability (e.g. intelligence/analytical pilots, reallocation of existing analytical assets, re-evaluation of analytical protocols and procedures, etc.) and will draft a fully justified budget request for increased analytical resources (e.g. more analysts, analytical software, etc.). By systematically applying criteria, performance gaps are more clearly identified and the scope of the gap is better defined, allowing fully justified and focused management attention, resource allocation, and budget requests.

(U) As the use of this system evolves, the IT Program will use historical information to accurately track progress. Basing program evaluation on the criteria for maximum feasible capability allows the IT Program to move away from TURK statistics, arrest and indictment statistics, individual cases, and international terrorist acts prevented to a more systematic and comprehensive identification of progress and capability. In addition to creating a performance measurement system, the use of criteria clearly communicates to IT Program managers (ADIC/SACs, Assistant Director, Deputy Assistant Director, Section Chiefs, Unit Chiefs, Supervisors) what is expected of them in the IT Program, providing a road map for program management. IT Program managers will then be able to specifically identify areas on which to focus management attention and resources nationally.

(U) The performance measurement system allows the use of both output measures (criteria) and outcome measures (capacity ratings) to provide a complete picture of the program and track progress. Once all the criteria have been evaluated and once capacity ratings have been determined, the IT Program will have valuable information at its disposal to use in decision and policy making, strategic resource allocation, communication (both internally and externally), and justification for budget requests. With full information constantly available, CTD's executive management will be able to make strategic decisions and develop a more coordinated national strategy. Significant issues that cut across field offices and programs will be more easily identified and, therefore, addressed in a more focused manner through comprehensive initiatives that maximize applicability and impact.

Data Collection, Verification, and Accountability

(U) The CTD has developed mechanisms to collect and verify information on the Five Levels criteria. For the field, the collection mechanism for the Level 1 Criteria will be the Annual Field Office Report (AFOR), which is submitted annually to FBI Headquarters by the field offices June 15. The criteria for Level 1 will be used as the IT Program's section of the AFOR beginning with the 2001 AFOR. An additional collection method will be through the ADIC/SACs written input into their six month performance appraisal progress report. From these two submissions from the Field, CTD will collect the criteria information on Level 1, as well as the ADIC/SAC capacity ratings (green, yellow, red). Validation of this information will occur through a CTD review of the submissions and a comparison with previous AFORs, Inspections, and the Director's Report on Counterterrorism. ADIC/SAC capacity ratings will be validated by the Assistant Director of CTD, in consultation with each ADIC/SAC. Accountability for progress towards maximum feasible capacity will be ensured through ADIC/SAC performance appraisals, the Deputy Director's SAC progress reviews, and through the Director's Report on Counterterrorism. All of these mechanisms for collection, verification, and accountability will be fully implemented in FY 2001.

(U) Collection, verification, and accountability mechanisms for Levels 2-5 (Headquarters-driven) have yet to be fully determined, but may include incorporation of criteria and capacity ratings into Section Chief performance appraisals, AD Contracts with the Deputy Director, and the Director's Report on Counterterrorism. For all levels, CTD is focusing on incorporating the performance measurement system into existing mechanisms instead of creating new systems and therefore more paperwork.

(U) The attached charts summarize criteria, performance measures, and data sources for each of the Five Levels in the IT Program. In addition, an attached summary document shows how outcome measures (capacity ratings) can be used to provide a snapshot of the FBI CT Program and progress towards maximum feasible capacity.

International Terrorism Program

Level 1: Field Capacity	Criteria	Performance Measure	Data Source
Base of Knowledge	1) Has the Division made staffing decisions relating to IT squads which reflect the Tier 1 nature of the IT program? 2) Has the Division ensured that all personnel on their Division's IT squad have attended all available IT related training appropriate to their experience level?	· % of Field Offices reporting appropriate numbers of dedicated IT personnel. · % of IT field personnel who have taken all available training	AFOR
% of Field Offices rated green in Base of Knowledge: xx% % of Field Offices rated yellow in Base of Knowledge: xx% % of Field Office rated red in Base of Knowledge: xx%			AFOR
Understanding of Local Environment	1)Has the Division built an intelligence base through active liaison and the development of quality sources? 2) Has the Division made decisions concerning the allocation of available translation resources which reflect the Tier 1 nature of the IT program? 3) Has the Division documented and disseminated an IT threat assessment (through the AFOR)? 4) Does the Division have a [redacted] or a formalized CT Working Group that addresses IT issues? 5)Has the Division participated in all relevant IT exercises?	· % of Field Offices reporting full utilization of intelligence gathering tools and opportunities. · % of [redacted] translated. · % of Field Offices that have documented and disseminated an IT threat assessment through the AFOR. · % of Field Offices with a [redacted] or formal CT Working Group. · % of relevant exercises in which Field Offices have participated.	AFOR
% of Field Offices rated green in Understanding of the Local Environment: xx% % of Field Offices rated yellow in Understanding of the Local Environment: xx% % of Field Office rated red in Understanding of the Local Environment: xx%			AFOR
Analytical Capabilities	1) Has the Division focused	· % of Field CT squads	AFOR

b7E

	analytical resources on providing tactical analytical services to the IT program?	reporting adequate analytical support.	
% of Field Offices rated green in Analytical Capabilities: xx% % of Field Offices rated yellow in Analytical Capabilities: xx% % of Field Office rated red in Analytical Capabilities: xx%			AFOR
Communication Capacity	1) Has the Division established and enforced a policy of maximizing information sharing with all appropriate FBI entities (within legal parameters) through the uploading and unblocking of IT case-related information?	% of case files not subject to legal exceptions that are uploaded and unblocked.	AFOR
% of Field Offices rated green in Communication Capacity: xx% % of Field Offices rated yellow in Communication Capacity: xx% % of Field Office rated red in Communication Capacity: xx%			AFOR
Disruption/ Offensive Initiatives	1) Has the Division established protocols to ensur[redacted] 2) Has the Division ensured that their Division's IT investigations focus on the development of human sources and the criminal prosecution of known terrorists.	% of [redacted]	AFOR
% of Field Offices rated green in Disruption/Offensive Initiatives: xx% % of Field Offices rated yellow in Disruption/Offensive Initiatives: xx% % of Field Office rated red in Disruption/Offensive Initiatives: xx%			AFOR
% of Field Offices rated green in IT: xx% % of Field Offices rated yellow in IT: xx% % of Field Offices rated red in IT: xx%			AFOR

b7E

Level 2: HQ Capacity	Criteria	Performance Measure	Data Source

Base of Knowledge	**1) Has the ITOS ensured that ITOS personnel have attended all available IT related training appropriate to their experience level?**	· **% of ITOS personnel who have attended all available training.**	**ITOS Assess-ment**
Rating of IT Section in Base of Knowledge: (green, yellow, red)			
Communication and Information Flow	**1) Has the ITOS developed the capability to extract pertinent, non-operational specific taskings from operational units?** **2) Has the ITOS implemented a "notes" protocol for sharing information between ITOS units?**	· **% of ITOS units briefed on the standardized process for fulfilling non-operational specific taskings (once such a process is developed).** · **% of ITOS personnel with access to and training in "notes" protocol.**	**ITOS Assess-ment**
Rating of IT Section in Communication and Information Flow: (green, yellow, red)			
Analytical Capabilities	**1) Has the ITOS acquired a tactical, analytical capacity for each ITOS operational unit?**	· **% of ITOS units reporting adequate analytical resources or with identified tactical analytical personnel in ISD.**	**ITOS Assess-ment**
Rating of IT Section in Analytical Capabilities: (green, yellow, red)			
Response and Direction to the Field	**1) Has ITOS articulated and encouraged the application of IT program priorities in the Field?** **2) Has the ITOS developed an IT threat assessment protocol for use by the Field?** **3) Has the ITOS developed an IT operational manual for use by both the Field and HQ personnel and ensured the timely and accurate updating of the Fugitive Handbook?** **4) Is the ITOS issuing daily threat reporting to the Field as well as regular communications updating the IT program's status?** **5) Has the ITOS dedicated management resources to the strategic planning process up to**	· **% of Field Offices that have access to IT program priorities and supporting documentation through the CTD website.** · **% of Field Offices that have received the IT threat assessment protocol.** · **% of Field Offices and HQ units that have received an IT operational manual (once developed) and updated Fugitive Handbook (once updated).** · **% of Field Offices that have access to ITOS daily threat reporting and regular communications updating the IT program's status through the CTD website.** · **% of IT executive**	**ITOS Assess-ment**

	and including the implementation phase?	**management reporting personal involvement in all phases of the strategic planning process.**	
Rating of IT Section in Response and Direction to the Field: (green, yellow, red)			
Overall Rating of the IT Section: (green, yellow, red)			

Level 3: FBI Capacity	Criteria	Performance Measure	Data Source
Assess	**1) Has the ITOS, in conjunction with the field, assessed the IT training opportunities which are currently available, including the IT portion of New Agents Training Course at Quantico? 2) Has the ITOS, in conjunction with the field, assessed the IT Program's needs vis-a-vis ISD (specifically the development and regular dissemination of tactical, analytical products for the field and the management and operations of SIOC)? 3) Has the ITOS assessed ITOS's facilities needs (specifically conference room and office space issues)? 4) Has the ITOS, in conjunction with the Field, assessed the needs of the IT program**	**% of support functions for which ITOS has conducted a comprehensive needs assessment.**	**ITOS Assess-ment**

	concerning the development of additional LEGAT offices overseas?		
Rating of CTD progress on IT program priorities in Assessment: (green, yellow, red)			
Articulate	1) Has the ITOS, in conjunction with the field, developed a method to accurately and consistently articulate the IT program's fiscal needs and priorities to the Finance Division? 2) Has the ITOS provided training assessment and recommendations to the Training Division? 3) Has the ITOS presented a proposed protocol for addressing analytical needs to ISD. 4) Has the ITOS articulated our facilities needs to ASD? 5) Has the ITOS presented findings concerning additional Legat offices to IRB? 6) Has the ITOS participated in monthly meetings of appropriate Assistant Directors to discuss IT needs and priorities? 7) Has the ITOS made field offices award of new research and development and new investigative techniques?	% of service divisions that have dedicated personnel assigned to address CT needs, as identified in comprehensive needs assessments.	ITOS Assess-ment
Rating of CTD progress on IT program priorities in Articulation: (green, yellow, red)			
Integrate	N/A, FY'00		
Rating of CTD progress on IT program priorities in Integration: (green, yellow, red)			
Evaluate	N/A, FY'00		
Rating of CTD progress on IT program priorities in Evaluation: (green, yellow, red)			
Overall Rating of CTD progress on IT Level 3 program priorities: (green, yellow, red)			

Level 4: Liaison Capacity	Criteria	Performance Measure	Data Source
Identify Partners	1) Has the ITOS, in conjunction with the field, prioritized current relationships with federal, state, and local agencies as well as foreign services and for restructuring the IT Program's method of fulfilling inter-agency requests to reflect those priorities?		ITOS Assess-ment
Rating of CTD progress on IT program priorities in Identifying Partners: (green, yellow, red)			
Establish Relationships	1) Has the ITOS maintained relationships with critical partners in order to ensure the continuing success of ITOSs Detailee Program?	· % of identified critical partners participating in the Detailee Program.	ITOS Assess-ment
Rating of CTD progress on IT program priorities in Establishing Relationships: (green, yellow, red)			
Mutual Needs Assessments	1) Has the ITOS assessed and articulated ITOS' interest in and need for the Attorney General's proposed "War Room/Translation Center"?		ITOS Assess-ment
Rating of CTD progress on IT program priorities in conducting Mutual Needs Assessments: (green, yellow, red)			
Information Sharing	1) Has the ITOS developed a program for briefing all out-going Ambassadors, Deputy Chiefs of Mission (DCM), Chiefs of Station (COS), and Deputy Chiefs of Station (DCOS) on ITOS program priorities and for briefing annual meetings of the same?	· % of outgoing Ambassadors briefed by ITOS on program priorities. · % of DCMs briefed by ITOS on program priorities. · % of COSs and DCOs briefed by ITOS on program priorities. · % of Ambassadors, DCMs, COSs, and DCOs participating in annual meetings that include	ITOS Assess-ment

		briefing by ITOS on program priorities.	
Rating of CTD progress on IT program priorities in Information Sharing: (green, yellow, red)			
Capability for Joint Product Development	1) Has the ITOS ensured the IT program's continuing participation in the FEST program and all related exercises?	% of FEST exercises in which the IT program participates.	ITOS Assess-ment
Rating of CTD progress on IT program priorities in Joint Product Development: (green, yellow, red)			
Overall Rating of CTD progress on IT Level 4 program priorities: (green, yellow, red)			

Level 5: Operations Capacity	Criteria	Performance Measure	Data Source
Command and Control Infrastructure	1) Has the ITOS, in conjunction with the field and other HQ divisions, developed and documented a SIOC organizational structure for all IT-interagency "specials"?		ITOS Assess-ment
Rating of CTD progress on IT program priorities in Command and Control Infrastructures: (green, yellow, red)			
Emergency Interagency Coordination Mechanisms	N/A, FY'00		
Rating of CTD progress on IT program priorities in Emergency Interagency Coordination Mechanisms: (green, yellow, red)			
Crisis-Based Resources	N/A, FY'00		
Rating of CTD progress on IT program priorities in Crisis-Based Resources: (green, yellow, red)			
Proactive, Coordinated Joint Operations	1) Has the ITOS, in conjunction with other federal agencies, developed an interagency system to develop and vet complex investigative initiatives such as terrorist fundraising investigations?	% of identified federal partners that participate in the development and maintenance of a system to develop and vet complex investigative initiatives.	ITOS Assess-ment
Rating of CTD progress on IT program priorities in Proactive, Coordinated Joint Operation: (green, yellow, red)			

Overall Rating of CTD progress on IT Level 5 program priorities: (green, yellow, red)	

Performance Measures Summary

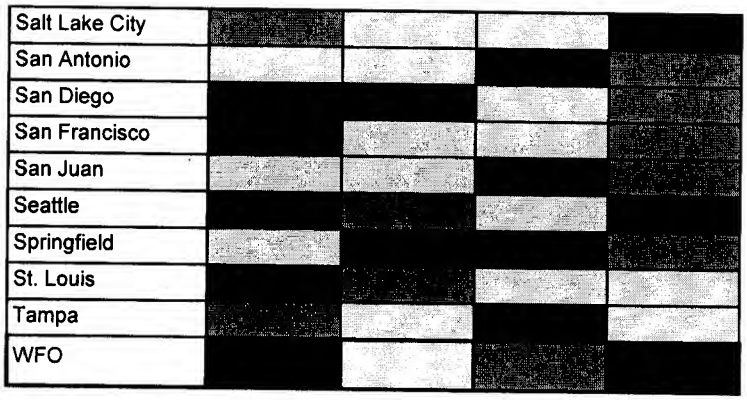
GREEN Maximum Feasible Capacity
YELLOW Vulnerable, making progress
RED Vulnerable, significant problems continuing

LEVEL 1: Field Capacity

Field Offices	GREEN	YELLOW	RED
Base of Knowledge	xx%	xx%	xx%
Understanding of the Local Environment	xx%	xx%	xx%
Analytical Capabilities	xx%	xx%	xx%
Communications Capacity	xx%	xx%	xx%
Disruption/Offensive Initiatives	xx%	xx%	xx%
Overall Rating	xx%	xx%	

Capacity Ratings By Field Office [FOR DISPLAY PURPOSES ONLY]

Field Office	NIPC	NDPO	IT	DT
Albany				
Albuquerque				
Anchorage				
Atlanta				
Baltimore				
Birmingham				
Boston				
Buffalo				
Charlotte				
Chicago				
Cincinnati				
Cleveland				
Columbia				
Dallas				
Denver				
Detroit				
El Paso				
Honolulu				
Houston				
Indianapolis				
Jackson				
Jacksonville				
Kansas City				
Knoxville				
Las Vegas				
Little Rock				
Los Angeles				
Louisville				
Memphis				
Miami				
Milwaukee				
Minneapolis				
Mobile				
Newark				
New Haven				
New Orleans				
New York				
Norfolk				
Oklahoma City				
Omaha				
Philadelphia				
Phoenix				
Pittsburgh				
Portland				
Richmond				
Sacramento				


Salt Lake City
San Antonio
San Diego
San Francisco
San Juan
Seattle
Springfield
St. Louis
Tampa
WFO

(Rev. 10-01-1999)

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY **Date:** 06/13/2000

To: All Divisions **Attn:** ADIC/SAC

From: Counterterrorism Division
Contact: [redacted] Ext. 4885 b6 b7C

Approved By: Pickard Thomas J
Watson Dale L

Drafted By: [redacted] sc

Case ID #: 66F-HQ-A1308701
66F-HQ-A1234210-K

Title: The Counterterrorism Division's Regional SAC Strategic Planning Conferences

Synopsis: This EC informs recipients of the above-captioned conferences.

Details: A Counterterrorism Task Force at FBIHQ, established and led by Assistant Director Dale Watson, with input from an SAC Advisory Board (to include SACs from CG, DL, PD, WFO, and KC), has developed a new management strategy for the Counterterrorism Program. During the months of July and August, 2000, the Counterterrorism Division (CTD) will conduct four regional conferences for ADICs and SACs to discuss the implementation of this new management strategy.

The conferences will be held in Jacksonville, Florida, on July 11th; Portland, Oregon, on July 25th; Washington, D.C., on August 1st; and Chicago, Illinois, on August 8th. During these conferences, AD Watson, in conjunction with the SACs from the advisory committee, will provide an overview of the new strategy and discuss the process for its implementation.

Each of the conferences will run from 9AM to 5:30PM and will take place on a Tuesday. Therefore, the Mondays prior to, and the Wednesdays following each conference will be considered travel days. It is only necessary for you to attend one of these conferences and each Division has been assigned a specific conference based on region. The regional assignments are as follows: **JACKSONVILLE, FL (July 11, 2000) -** Atlanta, Birmingham, Charlotte, Columbia, Dallas, Houston, Jackson, Jacksonville, Little Rock, Miami, Mobile, New Orleans, San Juan, San Antonio, and Tampa; **PORTLAND, OR (JULY 25, 2000) -** Anchorage, Albuquerque, Denver, El Paso, Honolulu, Las Vegas, Los Angeles, Phoenix, Portland, Sacramento, Salt Lake City, San

Diego, San Francisco, and Seattle; **WASHINGTON, D.C. (AUGUST 1, 2000)**-Albany, Baltimore, Boston, Buffalo, Newark, New York, New Haven, Norfolk, Philadelphia, Pittsburgh, Richmond, WFO; **CHICAGO, IL (AUGUST 8, 2000)**- Chicago, Cincinnati, Cleveland, Detroit, Indianapolis, Kansas City, Knoxville, Louisville, Memphis, Milwaukee, Minneapolis, Oklahoma City, Omaha, St. Louis, Springfield.

The TR number which will cover all four conferences is TR14CT000010. The Jacksonville conference will be held at the Sawgrass Marriott Resort, (800) 457 4653, where a block of rooms is being held. The hotel rate for Jacksonville is $65 a day, and the M&IE rate is $34 a day. The Portland conference will be held at the Portland Marriott City Center, (503) 226-6300, where a block of rooms is also being held. The hotel rate for Portland is $77 a day and the M&IE is $38 a day. Hotel information for Chicago and Washington will follow under a separate communication. The hotel rate for Chicago is $130 a day and the M&IE is $46 a day. The hotel rate for Washington, D.C. is $118 a day and the M&IE is $46 a day. Attire for all of these conferences will be business casual.

Please confirm your attendance at these conferences telephonically with [redacted] (202) 324-4885, by Friday, June 30, 2000. It is imperative that all SACs and ADICs attend one of these conferences. Therefore, if you have a conflict with the date to which you are currently assigned, please contact [redacted] concerning attending an alternate conference location. **Please note that each office is responsible for making their own hotel reservation.** In order to ensure that the number of attendees at all of the conferences remain manageable however, please be sure to confirm your attendance with [redacted] prior to making your hotel reservation.

b6
b7C

LEAD(s):

Set Lead 1: (Adm)

ALL RECEIVING OFFICES

Please confirm attendance with FBIHQ by Friday, June 30, 2000.

◆◆

(Rev. 08-28-2000)

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY **Date:** 04/24/2001

To: Counterterrorism **Attn:** DADs/Section Chiefs

From: Counterterrorism
CTD/Room 7110
Contact: [redacted] ext. 0759 b6 b7C

Approved By: Watson Dale L

Drafted By: [redacted]

Case ID #: 66F-HQ-A1308701

Title: **MAXCAP05**; THE COUNTERTERRORISM PROGRAM'S MANAGEMENT STRATEGY: LEVEL FIVE, PROGRAM MANAGEMENT

Synopsis: In conjunction with the new Counterterrorism Program Management Strategy, this communication provides CTD HQ Executive Management with specific guidance on the system which will be implemented in the coming weeks for defining and monitoring national strategies in the Counterterrorism Program.

Details: As you know, the CT Division is half-way through the first year of implementing its new five-level strategy for managing the program nationally. The field has successfully completed its first nation-wide self assessment results of which were compiled into the Director's Report on Counterterrorism last month (a program-specific summary was provided to each of you). Additionally, the CT portion of the 2001 AFOR has been completely reworked to focus on the Level 1 Criteria as laid out in the CT Strategy. The Counterterrorism Working Group has nearly completed the development of requirements for Levels 2-4 which encompass intelligence capacity, communications capacity, and liaison capacity and require substantial assistance and cooperation from other Headquarters Divisions.

While your participation in the development and implementation of all five levels is important, it is your active participation in the implementation of Level 5 which will be the decisive factor in the ultimate success or failure of the CT Strategy. As you will see, Level 5 is a system for rolling all of the input and information gathered from Levels 1-4 into clearly articulated,

prioritized, and monitored goals, objectives, and most importantly, strategies against the terrorist threat. In order to facilitate our ability to utilize this system, beginning in FY02, Section Chief contracts, which focus on the annual strategies of each of the CT Programs, will be instituted. With your help, we can increase our capacity to assess, monitor and effectively direct the CT Program.

To this end, in mid-May of this year, the CTD will be hosting a mandatory off-site conference for HQ Managers (details to follow). At this conference, the Level 5 system will be reviewed in detail, a further outline of what is required from every CTD Program Manager will be provided, your input and suggestions will be solicited, and the supporting technology will be demonstrated. This will provide you with the tools you need to fully implement this system for FY02.

Additionally, during the conference we will draft and prioritize interim strategies in each CT program area for the remainder of FY01. In order to achieve this, please have your Program Managers be prepared to discuss and prioritize their current programmatic strategies and proposed milestones for the remainder of FY01.

Level 5 requires Headquarters Program Managers to follow five specific phases throughout the fiscal year:

PHASE 1, ANNUAL ASSESSMENT: May-June Timeframe

Units Chiefs, in conjunction with program SSAs and IOSs, will complete an annual assessment of all of the program-specific input from Levels 1 through 4. The assessments will consist of detailed analysis of: Field Office assessments (AFORs) in Level 1; Intelligence Assessments in Level 2; Communication assessments (including inspection reporting) in Level 3; and Liaison Assessments in Level 4. Additionally, Unit Chiefs and their program managers will incorporate CTD Executive Management guidance provided from the DADs/AD into their program priorities for the coming year. Based on the review of all of these factors as they relate to their program areas, Unit Chiefs, in consultation with the Section Chiefs, will draft goals and priorities specific to their Program. These program strategies will include specific anticipated milestones, a detailed plan to attain their goals and milestones, and a listing of resources that will be required to attain the established priorities complete with supporting justification.

The enclosed form entitled "Counterterrorism Division FY ____ Program Priorities" illustrates the data fields that will be automated for input from each Unit/Section. Similar in fashion to

the AFOR, this automated document, as well as Section and Division level documents, will enable the Sections to articulate their use of Level 1-4 analysis to develop their programmatic goals, objectives, and strategies.

Level 1 analysis will be done through a review of the annual AFORs and the assessments of Level 2 through 4 will be conducted for all CTD programs as they apply. The form also provide for enumerating "Serious (non-resource related) program issues" that would affect successfully attaining maximum capacity in each of the CTD programs assessed. Non-resource issues could include legislative changes, intra-FBI procedural changes, intra-divisional issues, etc.

PHASE 2, PLANNING: June-July Time-frame

Next, during annual planning sessions, each Section's Section Chief and Unit Chiefs will present their proposed programmatic strategies and milestones for the coming fiscal year to the DAD and AD of Counterterrorism. This process will ensure early-on that each proposed program strategy is aligned with executive/national directives, and incorporates the required level of specificity. During these reviews, CT Program Managers will be expected to justify, with specificity, their proposed strategies and priorities based on the analysis of information gathered from Levels 1-4. At this time, the Program Managers will also explain their program's resource needs for the coming year and their plans to achieve their proposed milestones.

CTD Section Chiefs will incorporate the finalized, prioritized, Section goals and strategies which come out of these meetings into their Section Chief contracts for the upcoming year (the introduction of the Section Chief contract will begin in FY02). Further, program strategies and milestones will be the basis of the Section's Program Plan for the coming fiscal year and resource needs and supporting justification will be used for the section's budget formulation.

PHASE 3, DOCUMENTATION: August-October 1 (DEADLINE)

During Phase 3, the Section Chiefs/DADs will once again meet with the DADs and AD of Counterterrorism. This meeting will be used to establish the annual priorities for the National CT Program based on the finalized program priorities for each Section which came out of Phase 2.
The outcome of this meeting will be the finalized annual goals, priorities, strategies, and resource needs complete with supporting justification for the Counterterrorism Program for the coming year.

PHASE 4, MONITORING: ONGOING

Section Chiefs, in conjunction with their Unit Chiefs, SSAs and IOSs, will be responsible for establishing and maintaining mechanisms to monitor progress toward the program strategies and milestones established in the Section's annual program plan and the Section Chief contract.

PHASE 5, REVIEW: BIANNUAL (September and March)

Through a process of mid and end-of-year reviews of the Section Chief contracts by the DADs/AD of CTD, Section Chiefs will be responsible for reporting progress on their strategies and movement toward their program milestones.

This entire process will be supported by a user-friendly, electronic system (similar to the AFOR) which is currently under development. The plan is for this system to utilize the FBI Intranet, within security limitations, to allow multiple users access to a simple, and easily navigable database for inputting and prioritizing program goals, objectives, and strategies.

I appreciate your continuing partnership as we move forward with the full implementation of the new CT Strategy. As national Program Managers, it is through your successful implementation of Level 5 that the program will achieve maximum feasible capacity to counter the terrorism threat. I look forward to discussing this with you further at the May conference.

To: Counterterrorism From: Counterterrorism
Re: 66F-HQ-A1308701, 04/24/2001

COUNTERTERRORISM DIVISION

FY _____ UNIT/PROGRAM PRIORITIES

Priority Number _____
Section: _____ Unit/Program:_____
Unit Chief _____

Program Priority: All fields will be expandable to allow for complete documentation.
Analysis Supporting Level One Field Office Assessment:
Analysis Supporting Level Two Intelligence Assessment:
Analysis Supporting Level Three Communications Assessment:
Analysis Supporting Level Four Liaison Assessment
Planning for attainment of established goal:
Assessment of resource requirements for the goal:
Serious (non-resource related) program issues:

FY _____ SECTION PROGRAM GOALS

Section Chief _____

Goal Priority Number ___: Plan for attainment: Resource Requirements
Goal Priority Number ___: Plan for attainment: Resource Requirements

To: Counterterrorism From: Counterterrorism
Re: 66F-HQ-A1308701, 04/24/2001

Goal Priority Number ___:

Plan for attainment:

Resource Requirements

To: Counterterrorism From: Counterterrorism
Re: 66F-HQ-A1308701, 04/24/2001

FY _____ COUNTERTERRORISM DIVISION
PRIORITIES

Assistant Director: _____

Deputy Assistant Director: _____

Priority Number ___: Resource Requirements:
Priority Number ___: Resource Requirements:
Priority Number ___: Resource Requirements:
Priority Number ___: Resource Requirements:
Priority Number ___: Resource Requirements:

LEAD(s):

Set Lead 1: (Adm)

COUNTERTERRORISM

AT WASHINGTON, DC

(U) Review and prepare for the May CTD Headquarters Management Conference.

♦♦